US Government

Wireless Local Area Network (WLAN) Access System

Protection Profile

For

Basic Robustness Environments

INFORMATION
ASSURANCE
DIRECTORATE

April 07, 2004
Version 1.1

Table of Contents

List of Figures and Tables

Conventions and Terminology

Conventions

Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this PP are consistent with version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP reader.

The notation, formatting, and conventions used in this PP are largely consistent with those used in version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP user.

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this PP.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text*.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [Assignment_value].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

The **security target author** operation is used to denote points in which the final determination of attributes is left to the security target writer. Security target writer operations are indicated by the words “ST AUTHOR -”.

The CC paradigm also allows protection profile and security target authors to create their own requirements. Such requirements are termed ‘explicit requirements’ and are permitted if the CC does not offer suitable requirements to meet the authors’ needs. Explicit requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. In this PP, explicit requirements will be indicated with the “EXP” following the component name.

Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define “pass-fail” criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

NAMING CONVENTIONS

Assumptions: TOE security environment assumptions are given names beginning with “A.”-- e.g., A.ADMINISTRATION.

Threats: TOE security environment threats are given names beginning with “T.”-- e.g., T.SIGNAL_DETECT.

Policies: TOE security environment policies are given names beginning with “P.”—e.g., P.GUIDANCE.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with “O.” and “OE.”, respectively,—e.g., O.ACCESS and OE.ADMIN.

Terminology

In the CC, Section 2.3 of Part 1 defines many terms. In addition to terms defined in the CC, this PP references the following defined terms.

Access -- Interaction between an entity and an object that results in the flow or modification of data.

Access Control -- Security service that controls the use of resources[1] and the disclosure and modification of data.[2]

Access System --Equipment that provides the interface between mobile clients and the wired network.

Accountability -- Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator -- A user who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Assurance -- A measure of confidence that the security features of an IT system are sufficient to enforce its' security policy.

Asymmetric Cryptographic System -- A system involving two related transformations; one determined by a public key (the public transformation), and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key).

Asymmetric Key -- The corresponding public/private key pair needed to determine the behavior of the public/private transformations that comprise an asymmetric cryptographic system.

Attack -- An intentional act attempting to violate the security policy of an IT system.

Audit Server -- A central location where audit events/records are stored.

Authentication -- Security measure that verifies a claimed identity.

Authentication credentials -- Information used to verify a claimed identity.

[1] Hardware and software.

[2] Stored or communicated.

Authentication Server -- A central location where the users and administrators authentication credentials are stored.

Authorization -- Permission, granted by an entity authorized to do so, to perform functions and access data.

Authorized user -- An authenticated user who may, in accordance with the TSP, perform an operation.

Availability -- Timely[3], reliable access to IT resources.

Compromise -- Violation of a security policy.

Confidentiality -- A security policy pertaining to disclosure of data.

Critical Security Parameters (CSP) -- Security-related information (e.g., cryptographic keys, authentication data such as passwords and pins, and cryptographic seeds) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Cryptographic boundary -- An explicitly defined contiguous perimeter that establishes the physical bounds (for hardware) or logical bounds (for software) of a cryptographic module.

Cryptographic key (key) -- A parameter used in conjunction with a cryptographic algorithm that determines [7]:

- the transformation of plaintext data into cipher text data,
- the transformation of cipher text data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data, or
- a digital authentication code computed from data.

Cryptomodule – This Protection uses the term "cryptomodule" in several cryptographic functional requirements. When used this term has very specific meaning. It describes:

- a cryptographic module that is FIPS 140-1/2 validated (to comply with FCS_BCM_EXP);
- the cryptographic functionality implemented in that module are FIPS-approved security functions that have been validated; and

[3] According to a defined metric.

- the cryptographic functionality is available in a FIPS-approved mode for the cryptomodule.

Cryptographic Module -- The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Cryptographic Module Security Policy -- A precise specification of the security rules under which a cryptographic module must operate, including the rules derived from the requirements of this PP and additional rules imposed by the vendor.

Defense-in-Depth (DID) -- A security design strategy whereby layers of protection are utilized to establish an adequate security posture for an IT system.

Discretionary Access Control (DAC) -- A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. These controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Embedded Cryptographic Module -- A Cryptographic Module that is built as an integral part of a larger and more general surrounding system (i.e., one that is not easily removable from the surrounding system).

Enclave -- A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.

Entity -- A subject, object, user, or another IT device, which interacts with TOE objects, data, or resources.

External IT entity -- Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

Identity -- A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Integrity -- A security policy pertaining to the corruption of data and TSF mechanisms.

Integrity label -- A security attribute that represents the integrity level of a subject or an object. Integrity labels are used by the TOE as the basis for mandatory integrity control decisions.

Integrity level -- The combination of a hierarchical level and an optional set of non-hierarchical categories that represent the integrity of data.

MAC Address -- Media Access Control Address, the globally unique 48 bit media layer address of a network device. Sometimes referred to as the physical address.

Mandatory Access Control (MAC) -- A means of restricting access to objects based on subject and object sensitivity labels.[4]

Mandatory Integrity Control (MIC) -- A means of restricting access to objects based on subject and object integrity labels.

Multilevel -- The ability to simultaneously handle (e.g., share, process) multiple levels of data, while allowing users at different sensitivity levels to access the system concurrently. The system permits each user to access only the data to which they are authorized access.

Named Object[5] -- An object that exhibits all of the following characteristics:

- The object may be used to transfer information between subjects of differing user identities within the TSF.
- Subjects in the TOE must be able to request a specific instance of the object.
- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.

(Note: Due to the deletion of the last sentence in the OS PP (pertaining to intended use of the object being for sharing user data), something may need to be done to the requirements section of the PP (i.e., FDP_ACF) to ensure that some objects, which may satisfy the above but which are not intended for sharing user data do not need a full DAC implementation but rather it is acceptable if they are “owner only” or some other appropriate mechanism.)

Non-Repudiation -- A security policy pertaining to providing one or more of the following:

- To the sender of data, proof of delivery to the intended recipient,
- To the recipient of data, proof of the identity of the user who sent the data.

[4] The Bell LaPadula model is an example of Mandatory Access Control

[5] The only named objects in this PP, are operating system controlled files.

Object -- An entity within the TSC that contains or receives information and upon which subjects perform operations.

Operating Environment -- The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

Operating System (OS) -- An entity within the TSC that causes operations to be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects are exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security policies.

Operational key -- Key intended for protection of operational information or for the production or secure electrical transmissions of key streams.

Peer TOEs -- Mutually authenticated TOEs that interact to enforce a common security policy.

Public Object -- An object for which the TSF unconditionally permits all entities "read" access. Only the TSF or authorized administrators may create, delete, or modify the public objects.

Robustness -- A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DoD has three levels of robustness:

- **Basic:** Security services and mechanisms that equate to good commercial practices. Basic robustness equates to EAL-2 plus; ALC_FLR (Flaw Remediation), and AVA_MSU.1 (Misuse-Examination Guidance) as defined in CCIB-98-028, Part 3, Version 2.0

- **Medium:** Security services and mechanisms that provide for layering of additional safeguards above good commercial practices. Medium robustness equates to EAL-4 plus; ALC_FLR (Flaw Remediation); ADV_IMP.2; ADV_INT.1; ATE_DPT.2; and AVA_VLA.3 (Moderately Resistant Vulnerability Analysis) as defined in CCIB-98-028, Part 3, Version 2.0. If cryptographic functions are included in the TOE, then the PP should be augmented with AVA_CCA_EXP.2 as documented in the Protection Profile Medium Robustness Consistency Guidance.

- **High:** Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

Secure State -- Condition in which all TOE security policies are enforced.

Security attributes -- TSF data associated with subjects, objects, and users that is used for the enforcement of the TSP.

Security level -- The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity on the information [10].

Sensitivity label -- A security attribute that represents the security level of an object and that describes the sensitivity (e.g. Classification) of the data in the object. Sensitivity labels are used by the TOE as the basis for mandatory access control decisions [10].

Split key -- A variable that consists of two or more components that must be combined to form the operational key variable. The combining process excludes concatenation or interleaving of component variables.

Subject -- An entity within the TSC that causes operations to be performed.

Symmetric key -- A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms.

Threat -- Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

Threat Agent - Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.

TOE Security Function (TSF) Data -- Information used by the TSF in making TOE security policy (TSP) decisions. TSF data may be influenced by users if allowed by the TSP. Security attributes, authentication data, and access control list entries are examples of TSF data.

Unauthorized User -- Any person who is not authorized, under the TSP, to access the TOE. This definition authorized users who seek to exceed their authority.

User -- Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User Data -- Data created by and for the authorized user that does not affect the operation of the TSP. User data is separate from the TSF data, which has security attributes associated with it and the system data.

Vulnerability -- A weakness that can be exploited to violate the TOE security policy.

Wireless Client -- A device consisting of hardware and software used to provide a wirelessly interface to communicate with other wireless devices.

Document Organization

Section 1 provides the introductory material for this PP. It includes an introduction, a brief description of the WLAN access system TOE and additional identifying information. It also includes a discussion of the factors used to define the TOE environment and the level of Robustness selected for this PP.

Section 2 describes, in detail, the WLAN access system TOE (i.e., the TOE for this PP) and the IT environment upon which the TOE depends.

Section 3 describes the TOE security environment. This includes:

- Secure-use assumptions that describe the presumptive conditions for secure use of the TOE in the a basic robustness environment
- Threats that are to be addressed either completely or partially by the technical countermeasures implemented in the WLAN access system.
- Organizational policies that levy further requirements on the TOE.

In addition this section also identifies those threats and policies that are defined as part of the basic robustness environment that the WLAN access system does not address.

Section 4 defines the security objectives for the WLAN access system in a basic robustness environment.

Section 5 contains the functional and assurance requirements derived from the CC, Parts 2 and 3, respectively that must be satisfied by the WLAN access system. This section also identifies requirements that are levied on the TOE IT environment.

Section 6 provides a rationale to demonstrate that the information technology security objectives for the TOE and its IT environment satisfy the identified policies and threats. The section then provides rationale to show that the set of requirements are sufficient to meet each objective, and that each security objective is addressed by one or more component requirements. Therefore, the two aforementioned subsections provide arguments that the security objectives and security requirements are both necessary and sufficient, respectively and collectively, to meet the needs dictated by the policies and threats. Section also 6 provides arguments that to address any unsatisfied dependencies, and the selected strength of function.

Section 7, Identifies references to noteworthy background and/or supporting materials.

Appendix A is an acronym list that defines frequently used acronyms.

1. Introduction

This Protection Profile (PP) supports future Department of Defense (DoD) procurements of commercial off-the-shelf (COTS) wireless local area network (WLAN) access system components that will be used in basic robustness environments. This PP details the policies, assumptions, threats, security objectives, security functional requirements, and security assurance requirements for the WLAN access point and its supporting environment.

This PP has two primary audiences: Information System Security Engineers (ISSE) and COTS WLAN access system product vendors. The ISSE may use this PP to help in designing and assessing installations in which COTS WLAN access system devices are part of the information system. WLAN product vendors will use the PP to learn the DoD security requirements for new COTS WLAN devices being procured.

1.1 Identification

Title:	US Government Wireless Local Area Network (WLAN) Access System For Basic Robustness Environments Protection Profile
Version:	1.1
Sponsor:	National Security Agency (NSA)
CC Version:	Common Criteria (CC) Version 2.1, and applicable interpretations.
Evaluation Level:	Evaluation Assurance Level (EAL) 2 augmented with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), and AVA_MSU.1 (Misuse – Examination of Guidance).
Keywords:	Access system, basic robustness, radio, wireless, network, wireless local area network, wireless LAN, WLAN, LAN

1.2 Protection Profile Overview

This PP specifies the minimum-security requirement for a WLAN Access System (hereafter referred to as the Target of Evaluation (TOE) used by the US Government in Basic Robustness Environments. The target robustness level of "basic" is specified in the *Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG*).

This PP requires privacy and integrity of communications over the WLAN, using commercially available cryptographic algorithms. Security administration at the access system is also a requirement. The assurance requirements specified in the PP are EAL 2 augmented with flaw remediation, assurance maintenance and misuse analysis.

This PP defines:

- assumptions about the security aspects of the environment in which the TOE will be used;
- threats that are to be addressed by the TOE;
- security objectives of the TOE and its environment
- functional and assurance requirements to meet those security objectives; and
- rationale demonstrating how the requirements meet the security objectives.

1.3 TOE Environment Defining Factors

In trying to specify the environments in which TOEs with various levels of robustness are appropriate, it is useful to first discuss the two defining factors that characterize that environment: **value of the resources** and **authorization of the entities** to those resources.

In general terms, the environment for a TOE can be characterized by the authorization (or lack of authorization) the least trustworthy entity has with respect to the highest value of TOE resources (i.e. the TOE itself and all of the data processed by the TOE).

Note that there are an infinite number of combinations of entity authorization and value of resources; this conceptually “makes sense” because there are an infinite number of potential environments, depending on how the resources are valued by the organization, and the variety of authorizations the organization defines for the associated entities. In the next section 1.3.1, these two environmental factors will be related to the robustness required for selection of an appropriate TOE.

1.3.1 Value of Resources

Value of the resources associated with the TOE includes the data being processed or used by the TOE, as well as the TOE itself (for example, a real-time control processor). “Value” is assigned by the using organization. For example, in the DoD low-value data might be equivalent to data marked “FOUO”, while high-value data may be those classified Top Secret. In a commercial enterprise, low-value data might be the internal organizational structure as captured in the corporate on-line phone book, while high-value data might be corporate research results for the next generation product. Note that when considering the value of the data one must also consider the value of data or resources that are accessible through exploitation of the TOE. For example, a firewall may have “low value” data itself, but it might protect an enclave with high value data. If the firewall was being depended upon to protect the high value data, then it must be treated as a high-value-data TOE.

1.3.2 Authorization of Entities

Authorization that entities (users, administrators, other IT systems) have with respect to the TOE (and thus the resources of that TOE, including the TOE itself) is an abstract concept reflecting a combination of the trustworthiness of an entity and the access and privileges granted to that entity with respect to the resources of the TOE. For instance, entities that have total authorization to all data on the TOE are at one end of this spectrum; these entities may have privileges that allow them to read, write, and modify anything on the TOE, including all TSF data. Entities at the other end of the spectrum are those that are authorized to few or no TOE resources. For example, in the case of a router, non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources. In the case of an OS, an entity may not be allowed to log on to the TOE at all (that is, they are not valid users listed in the OS's user database)**.**

It is important to note that authorization **does not** refer to the **access** that the entities actually have to the TOE or its data. For example, suppose the owner of the system determines that no one other than employees was authorized to certain data on a TOE, yet they connect the TOE to the Internet. There are millions of entities that are not **authorized** to the data (because they are not employees), but they actually have connectivity to the TOE through the Internet and thus can attempt to access the TOE and its associated resources.

Entities are characterized according to the value of resources to which they are authorized; the extent of their authorization is implicitly a measure of how trustworthy the entity is with respect to compromise of the data (that is, compromise of any of the applicable security policies; e.g., confidentiality, integrity, availability). In other words, in this model the greater the extent of an entity's authorization, the more trustworthy (with respect to applicable policies) that entity is.

1.3.3 Selection Of Appropriate Robustness Levels

Robustness is a characteristic of a TOE defining how well it can protect itself and its resources; a more robust TOE is better able to protect itself. This section relates the defining factors of IT environments, authorization, and value of resources to the selection of appropriate robustness levels.

When assessing any environment with respect to Information Assurance the critical point to consider is the likelihood of an attempted security policy compromise, which was characterized in the previous section in terms of entity authorization and resource value. As previously mentioned, robustness is a characteristic of a TOE that reflects the extent to which a TOE can protect itself and its resources. It follows that as the likelihood of an attempted resource compromise increases, the robustness of an appropriate TOE should also increase.

It is critical to note that several combinations of the environmental factors will result in environments in which the likelihood of an attempted security policy compromise is similar. Consider the following two cases:

The first case is a TOE that processes only low-value data. Although the organization has stated that only its employees are authorized to log on to the system and access the data, the system is connected to the Internet to allow authorized employees to access the system from home. In this case, the least trusted entities would be unauthorized entities (e.g. non-employees) exposed to the TOE because of the Internet connectivity. However, since only low-value data are being processed, the likelihood that unauthorized entities would find it worth their while to attempt to compromise the data on the system is low and selection of a basic robustness TOE would be appropriate.

The second case is a TOE that processes high-value (e.g., classified) information. The organization requires that the TOE be stand-alone, and that every user with physical and logical access to the TOE undergo an investigation so that they are authorized to the highest value data on the TOE. Because of the extensive checks done during this investigation, the organization is assured that only highly trusted users are authorized to use the TOE. In this case, even though high value information is being processed, it is unlikely that a compromise of that data will be attempted because of the authorization and trustworthiness of the users and once again, selection of a basic robustness TOE would be appropriate.

The preceding examples demonstrated that it is possible for radically different combinations of entity authorization/resource values to result in a similar likelihood of an attempted compromise. As mentioned earlier, the robustness of a system is an indication of the protection being provided to counter compromise attempts. Therefore, a basic robustness system should be sufficient to counter compromise attempts where the likelihood of an attempted compromise is low. The following chart depicts the "universe" of environments characterized by the two factors discussed in the previous section: on one axis is the authorization defined for the least trustworthy entity, and on the other axis is the highest value of resources associated with the TOE.

As depicted in the following figure, the robustness of the TOEs required in each environment steadily increases as one goes from the upper left of the chart to the lower right; this corresponds to the need to counter increasingly likely attack attempts by the least trustworthy entities in the environment. Note that the shading of the chart is intended to reflects the notion that different environments engender similar levels of "likelihood of attempted compromise", signified by a similar color. Further, the delineations between such environments are not stark, but rather are finely grained and gradual.

While it would be possible to create many different "levels of robustness" at small intervals along the "Increasing Robustness Requirements" line to counter the increasing likelihood of attempted compromise due to those attacks, it would not be practical nor particularly useful. Instead, in order to implement the robustness strategy where there are only three robustness levels: Basic, Medium, and High, the graph is divided into three sections, with each section corresponding to set of environments where the likelihood of attempted compromise is roughly similar. This is graphically depicted in the following chart.

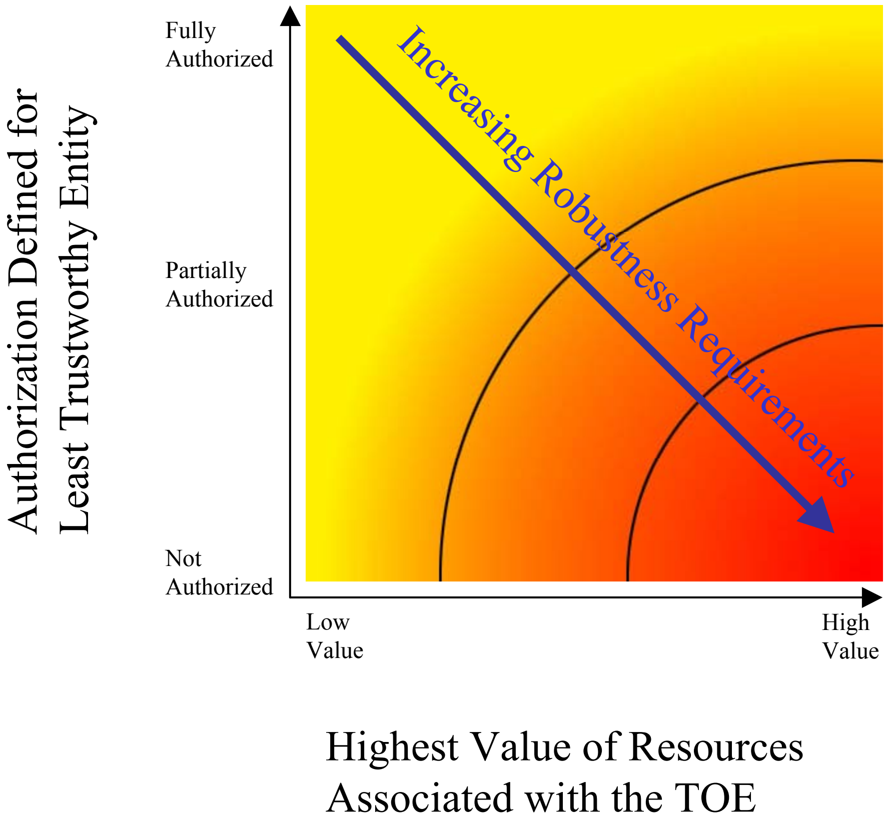

Figure 1: Value of TOE Resources vs. Trust

In this second representation of environments and the robustness plane below, the "dots" represent given instantiations of environments; like-colored dots define environments with a similar likelihood of attempted compromise. Correspondingly, a TOE with a given robustness should provide sufficient protection for environments characterized by like-colored dots. In choosing the appropriateness of a given robustness level TOE PP for an environment, then, the user must first consider the lowest authorization for an entity as well as the highest value of the resources in that environment. This should result in a "point" in the chart above, corresponding to the likelihood that that entity will attempt to compromise the most valuable resource in the environment. The appropriate robustness level for the specified TOE to counter this likelihood can then be chosen.

The difficult part of this activity is differentiating the authorization of various entities, as well as determining the relative values of resources; (e.g., what constitutes "low value" data vs. "medium value" data). Because every organization will be different, a rigorous definition is not possible. In section 3 of this PP, the targeted threat level for a basic robustness TOE is characterized. This information is provided to help organizations using this PP insure that the functional requirements specified by this basic robustness PP are appropriate for their intended application of a compliant TOE.

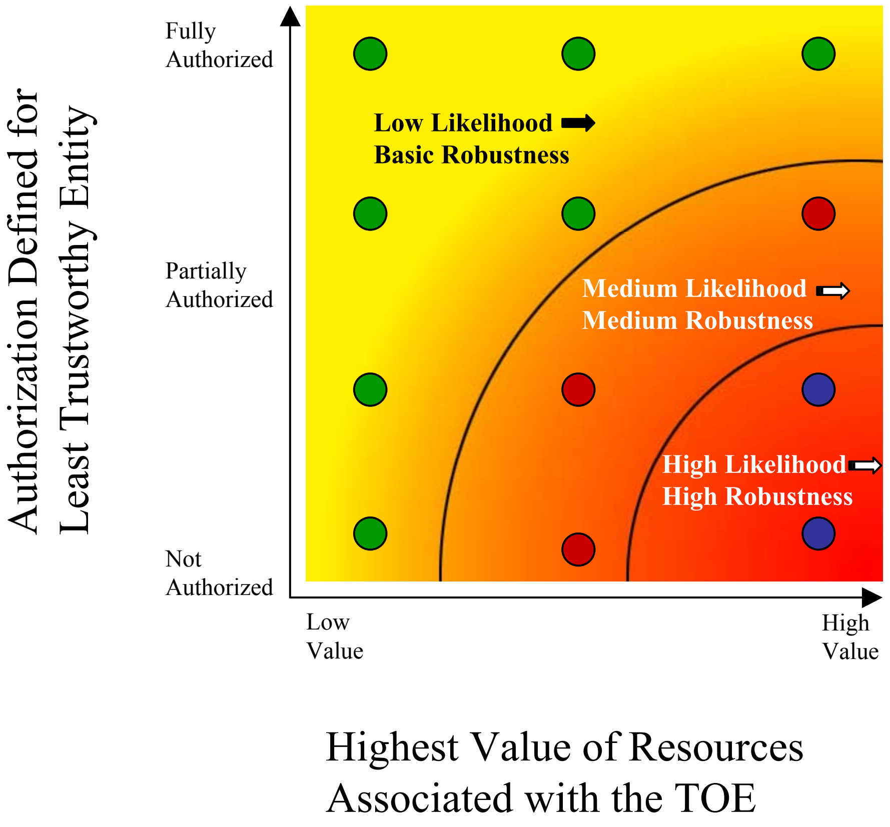

Figure 2: Value of TOE Resources vs. Robustness

1.4 Related Protection Profiles

This Profile is part of planned set of Protection Profiles for wireless communications. It is related to a previously distributed draft Protection Profile titled *Infrastructure Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments Protection Profile, Version 0.6, dated September 28, 2001* The completed set of Protection Profiles replaces that draft Protection Profile.

2. TOE Description

The Target of Evaluation (TOE) is a wireless LAN access system. A wireless LAN access system can be defined as one or more components that provide secure wireless access to a wired or wireless network. For the purpose of this PP we will be discussing a typical wired to wireless configuration. However the reader should keep in mind that it does not preclude any other wireless configuration that may exist. This TOE may vary in the type of components used to provide access to the wired LAN. This PP does not dictate a particular configuration. Instead the PP addresses the security requirements for the system that allows access to the wired network while performing management functions within the system. The security requirements of the TOE are identification and authentication (I&A), audit, encryption, information flow control, and administration.

A WLAN is an extension, or possibly a replacement, of a traditional wired network. It allows mobile, wireless clients to be roaming hosts on the network, and to connect to the network using access points. The traditional wireless LAN is set up as in Figure 3. In the typical configuration, an Access Point (AP) controls the establishment of the link between wireless clients and the AP itself. The AP is a communications infrastructure device that provides network connectivity to mobile clients. As such, it is not intended to provide any direct network services to the users that connect through the AP. The AP relies mainly on the environment in which it resides to perform many of the management duties and providing secure access to the network and does not offer a great deal of security. Therefore, with current products, it is almost always necessary to implement a layered solution by overlaying additional components in order to meet security requirements listed in this PP.

Most WLAN AP’s do not meet the security requirements mentioned in this PP. For example APs can implement a security policy that restricts wireless clients to a set of administrator defined MAC address. However there are many documented attacks that can defeat MAC address authentication. In addition, Wired Equivalent Privacy (WEP) enabled APs are prone to attacks due to the nature of the encryption algorithm that it uses. It is now necessary to incorporate additional devices that will provide secure access control components to the network. These layered solutions (e.g., VPN, Wireless Gateway, Wireless Security Switch) are all valid as deployment architectures for a wireless access system compliant with this PP. There are various combinations of components that allow for a secure access to the wired network. In the future it may be possible to provide one or all types of architectures in a single system that includes the AP’s and this will be designed to meet the expectations of this PP. When this happens, the use of a layered solution will be optional if the AP meets this PP.

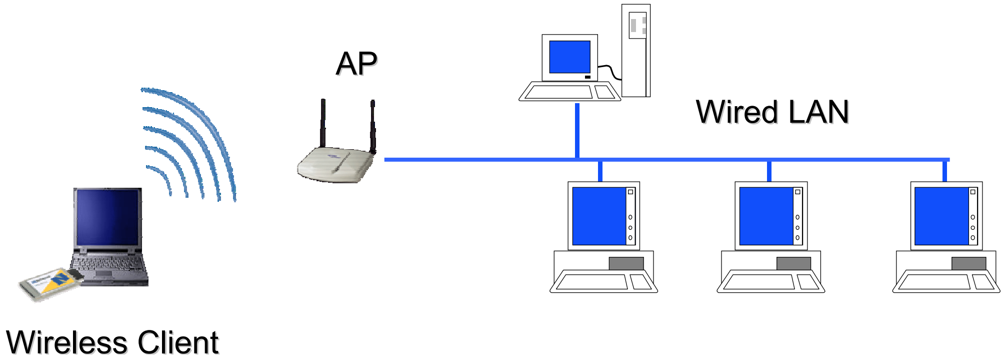

Figure 3: Traditional Wireless LAN

2.1 TOE Functionality

Wireless LAN access systems include necessary management and security functions to operate in accordance with this PP. The TOE includes applications that provide management capabilities, auditing functions, and authentication features. In protecting the network, the system addresses security at either Layer 2 (Link Layer) or Layer 3 (Network Layer) or both.

The functionality of a wireless access system *may* be implemented by more than one physical component. Figure 4 shows an example of a WLAN using an access system architecture. As stated in Section 2.0, AP's provide network connectivity to mobile clients and does not provide direct network services to the user. Therefore, the access system can be the layered solution that will include the AP. It should be noted that an AP, which is not represented in Figure 4, could be included between the wireless client and the access system to provide the network connectivity to the user. The PP specifies the functional and security requirements for a system as a whole and does not attempt to separate requirements by component. In all cases, wireless traffic must be able to pass to the wired network via the wireless access system providing the necessary security. This PP will address environmental requirements on both the wired network and the wireless access system.

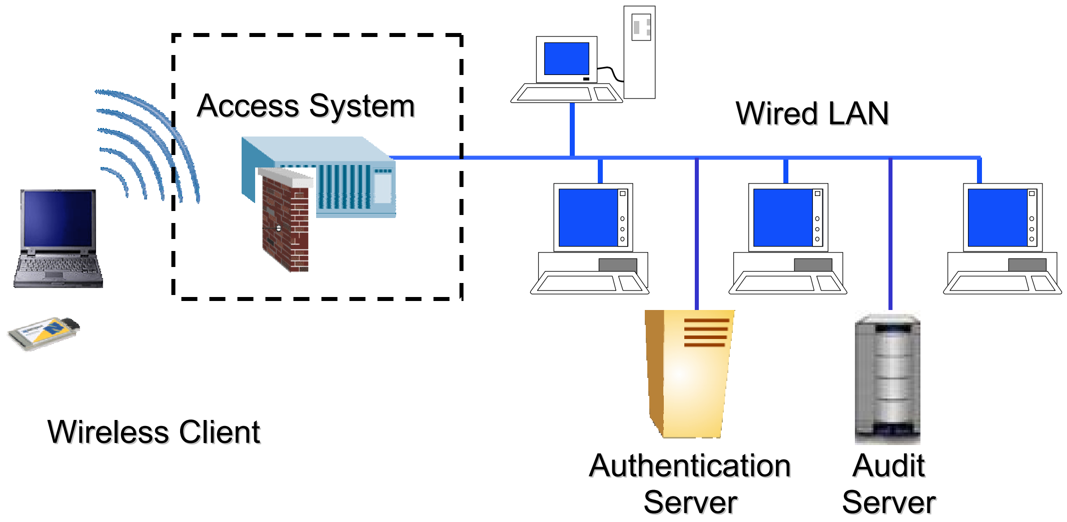

Figure 4: Example of WLAN using an access system architecture with an Authentication server and Audit Server

2.2 Identification and Authentication

The TOE requires that administrators be properly identified and authenticated prior to performing any administrative tasks for the TOE. However, the TOE provides for multiple Identification and Authentication (I&A) mechanisms for access to services residing on the TOE or for services mediated by the TOE. The type of authentication mechanism required depends on the origin of the source (i.e., remote user from the wireless environment, remote administrative user from the wired environment, or administrative user from a TOE console) requesting the service. The authentication of a user will be based on a set of authentication credentials assigned to each user. A Unix style user ID and password is an example of authentication credentials to the TOE. A Unix style user ID and password is also sufficient for administrative access to the TOE from the wired network.

The TOE also requires that the individual or user be authenticated prior to the access system. A remote authentication server is used to also perform the authentication of the individual user as well as the administrator. Although the authentication server is outside of the TOE and resides in the environment, requirements should be specified for secure communication between the TOE and the authentication server and the audit server.

2.3 Administration

"Administrators" refers to the roles assigned to the individuals responsible for the installation, configuration, and maintenance of the TOE. The administrative role includes cryptographic administration, audit administration and security administration. Cryptographic administration covers the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the TOE. Audit administration covers the establishment of audit criterion and the regular review of the TOE's audit data. The TOE environment performs the review of the TOE's audit data. Security administration includes all other administrative tasks (e.g., creating the TOE security policy) not addressed by the other two administrative areas. While this PP describes the three types of administrative responsibilities outlined above, it provides the ST author the option of incorporating all three types of administrative activities under a single role or including additional administrative roles as well.

2.4 Information Flow Control

One of the ways that the TOE enforces information flow is by requiring the establishment of an encrypted communications channel. The TOE may further restrict potential flows by granting or denying access to the network based upon authentication by a remote server. The TOE requires secure communication to both the authentication and the audit servers.

2.5 Encryption

This TOE includes requirements for cryptographic modules. Those modules must comply with Federal Information Processing Standard Publication (FIPS PUB) 140-1/2, which defines security requirements for cryptographic modules. A cryptographic module is that part of a system or application that provides cryptographic services, such as encryption, authentication, or electronic signature generation and verification. Products and systems compliant with this PP are expected to utilize cryptographic modules compliant with this FIPS PUB. FIPS PUB 140-2 has superceded FIPS PUB 140-1 however the DoD recognizes those products that currently hold the validation. For the purposes of this PP, FIPS PUB 140-1 will be accepted and it should be noted that no product will be validated against FIPS PUB 140-1 if it was not certified prior to being superceded by FIPS PUB 140-2.

2.6 Audit

The TOE can generate auditable events, audit records, and audit management itself or it can work in cooperation with its IT environment. It is expected that the IT environment will provide the mechanisms for audit event storage and retrieval. Table 9 in the FAU_GEN.1-NIAP-0410 requirement, lists the minimum set of auditable events that must be available to the Security Administrator for configuration on the TOE. Each auditable event must generate an audit record. Table 9 also provides a minimum list of attributes that must be included in each audit record. The Security Target (ST) author may include additional auditable events and audit record attributes. If the ST author includes any additional functional requirements not specified by this PP, they must consider any security relevant events associated with those requirements and include them in the TOE's list of auditable events and records.

3. TOE Security Environment

The TOE specified within this PP is intended for use in basic robustness environments. Basic robustness TOEs fall in the upper left area of the previously discussed robustness figures. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in "good commercial practices" that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE.

Threat agent motivation can be considered in a variety of ways. One possibility is that the value of the data process or protected by the TOE will generally be seen as of little value to the adversary (i.e., compromise will have little or no impact on mission objectives). Another possibility, (where higher value data is processed or protected by the TOE) is that procuring organizations will provide other controls or safeguards (i.e., controls that the TOE itself does not enforce) in the fielded system in order to increase the threat agent motivation level for compromise beyond a level of what is considered reasonable or expected to be applied.

The remainder of this chapter (Chapter 3) describes the assumptions, threats, and policies that are relevant to both the WLAN TOE and the WLAN TOE environment. The first section describes the Secure Usage Assumptions—these are the assumptions that support the secure use of the WLAN. Threats are countered by the security objectives. Policies support the security objectives and are used by security objectives to counter threats.

3.1 Secure Usage Assumptions

Assumptions are limiting conditions that are accepted before developing policy or considering threats. Table 1: TOE Assumptions identifies the conditions that are assumed to exist in the operational environment. In addition to the standard list of assumptions for Basic Robustness Protection Profiles, there are two assumptions that deal with the special roles of remote administration/management and audit servers in this PP.

Table 1: TOE Assumptions

Name	Assumption
A.AUDIT	The environment shall provide the capability to protect audit information and authentication credentials. The environment shall also provide the capability to selectively view audit information.
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.
A.PROTECT_MGMT_COMMS	The environment shall protect the transport of audit records to the audit server and the backside network management

	communications with the TOE in a manner that is commensurate with the risks posed to the protected network. The environment will also protect the communication between the TOE and the authentication server.
A.TOE_NO_BYPASS	Information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

3.2 Threats to Security

The threats listed in Table 2: Threats are general threats. Threats are actions that may have an adverse affect on the Basic Robustness WLAN or mission. Exposure of wireless communications in the RF transmission environment introduces unique threats for the WLAN. The WLAN interconnected to a wired network could effectively create a hole in the wired infrastructure boundary because it exposes information to the RF medium where signals can be more readily detected and intercepted. With WLANs, an adversary no longer requires physical access to the network to exploit a wireless system. For basic robustness, the threats identified do not include those that would be considered a sophisticated attack (e.g., intentional jamming, traffic analysis).

In addition to helping define the robustness appropriate for a given environment, the threat agent is a key component of the formal threat statements in the PP. Threat agents are typically characterized by a number of factors such as *expertise*, *available resources*, and *motivation*. Because each robustness level is associated with a variety of environments, there are corresponding varieties of specific threat agents (that is, the threat agents will have different combinations of motivation, expertise, and available resources) that are valid for a given level of robustness. The following discussion explores the impact of each of the threat agent factors on the ability of the TOE to protect itself (that is, the robustness required of the TOE).

The *motivation* of the threat agent seems to be the primary factor of the three characteristics of threat agents outlined above. Given the same expertise and set of resources, an attacker with low motivation may not be as likely to attempt to compromise the TOE. For example, an entity with no authorization to low value data none-the-less has low motivation to compromise the data; thus a basic robustness TOE should offer sufficient protection. Likewise, the fully authorized user with access to highly valued data similarly has low motivation to attempt to compromise the data, thus again a basic robustness TOE should be sufficient.

Unlike the motivation factor, however, the same can't be said for *expertise*. A threat agent with low motivation and low expertise is just as unlikely to attempt to compromise a TOE as an attacker with low motivation and high expertise; this is because the attacker with high expertise does not have the motivation to compromise the TOE even though they may have the expertise to do so. The same argument can be made for *resources* as well.

Therefore, when assessing the robustness needed for a TOE, the motivation of threat agents should be considered a "high water mark". *That is, the robustness of the TOE should increase as the motivation of the threat agents increases.*

Having said that, the relationship between expertise and resources is somewhat more complicated. In general, if resources include factors other than just raw processing power (money, for example), then expertise should be considered to be at the same "level" (low, medium, high, for example) as the resources because money can be used to purchase expertise. Expertise in some ways is different, because expertise in and of itself does not automatically procure resources. However, it may be plausible that someone with high expertise can procure the requisite amount of resources by virtue of that expertise (for example, hacking into a bank to obtain money in order to obtain other resources).

It may not make sense to distinguish between these two factors; in general, it appears that the only effect these may have is to lower the robustness requirements. For instance, suppose an organization determines that, because of the value of the resources processed by the TOE and the trustworthiness of the entities that can access the TOE, the motivation of those entities would be "medium". This normally indicates that a medium robustness TOE would be required because the likelihood that those entities would attempt to compromise the TOE to get at those resources is in the "medium" range. However, now suppose the organization determines that the entities (threat agents) that are the least trustworthy have no resources and are unsophisticated. In this case, even though those threat agents have medium motivation, the likelihood that they would be able to mount a successful attack on the TOE would be low, and so a basic robustness TOE may be sufficient to counter that threat.

It should be clear from this discussion that there is no "cookbook" or mathematical answer to the question of how to specify exactly the level of motivation, the amount of resources, and the degree of expertise for a threat agent so that the robustness level of TOEs facing those threat agents can be rigorously determined. However, an organization can look at combinations of these factors and obtain a good understanding of the likelihood of a successful attack being attempted against the TOE. Each organization wishing to procure a TOE must look at the threat factors applicable to their environment; discuss the issues raised in the previous paragraph; consult with appropriate accreditation authorities for input; and document their decision regarding likely threat agents in their environment.

The important general points we can make are:

- The motivation for the threat agent defines the upper bound with respect to the level of robustness required for the TOE
- A threat agent's expertise and/or resources that is "lower" than the threat agent's motivation (e.g., a threat agent with high motivation but little expertise and few resources) may lessen the robustness requirements for the TOE (see next point, however).
- The availability of attacks associated with high expertise and/or high availability of resources (for example, via the Internet or "hacker chat rooms") introduces a problem when trying to define the expertise of, or resources available to, a threat agent.

Table 2: Threats

Threat Name	Threat Definition
T.ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective

Threat Name	Threat Definition
	security mechanisms.
T.ACCIDENTAL_ CRYPTO_ COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.
T.UNAUTHORIZED_ ACCESS	A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
T.UNAUTH_ADMIN_ACCESS	An unauthorized user or process may gain access to an administrative account.
T.UNIDENTIFIED_ ACTIONS	The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.

Table 3: Basic Robustness Threats NOT Applicable to the TOE

Threat Name	Threat Definition	Rationale for NOT Including this Threat
T.ACCIDENTAL_AUDIT_COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	The storage/retrieval and review of audit records is provided by the IT environment. Hence, although this threat must be addressed within the IT environment, the functional requirements specified in this PP do not provide the functionality required to protect the audit records in the external environment. Although there may be some cases where one could argue that requiring encrypted RF communications and user authentication will assist in addressing this threat. The fundamental threat must be met by protecting communications path that the audit records travel for storage and review.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 4: Organizational Security Policies identifies the organizational security policies applicable to the WLAN.

Table 4: Organizational Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
P.ENCRYPTED_CHANNEL	The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
P.NO_AD_HOC_NETWORKS	In concordance with the DOD Wireless Policy, there will be

	no ad hoc 802.11 or 802.15 networks allowed.

3.4 Security Function Policies

Several of the functional requirements in section 5.1 reference Security Function Policies (SFPs). SFPs are named pieces of requirements. They are no organizational policies. Each SFP is listed in the table below with an explanation that supplies additional information and interpretation.

Table 5: Security Function Policies

Policy Name	Policy Definition
P.SPECIFIED USERS SFP	The access system administrators shall specifically identify the set of wireless clients that can connect to the network through the remote access server. The TSF shall filter traffic at the wireless interfaces based upon the user authentication credentials stored in the authentication server. The traffic across the wired side of the network is not directly restricted by the information flow control policy.
P.WIRELESS ENCRYPTION SFP	The users/access system administrators shall specify that the TOE encrypt/decrypt user data as it transits to/from wireless network.

4. Security Objectives for the TOE

Table 6: Security Objectives for the TOE identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. The table also shows the corresponding threats and policies that are addressed by the objectives. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 6: Security Objectives for the TOE

Name	TOE Security Objective
O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events.
O.CONFIGURATION_IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.
O.CORRECT_ TSF_OPERATION	The TOE will provide the capability to verify the correct operation of the TSF.
O.CRYPTOGRAPHY	The TOE shall use NIST FIPS 140-1/2 validated cryptographic services.
O.DISPLAY_BANNER	The TOE will display an advisory warning prior to establishing an administrator session regarding use of the TOE prior to permitting the use of any TOE services that requires authentication.
O.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.
O.MANAGE	The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.
O.PARTIAL_FUNCTIONAL_ TESTING	The TOE will undergo security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
O.RESIDUAL_ INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.

Name	TOE Security Objective
O.SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.TIME_STAMPS	The TOE will provide reliable time stamps and the capability for the administrator to set the time used for these time stamps
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.VULNERABILITY_ANALYSIS	The TOE will undergo vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.

4.1 Security Objectives for the Environment

The assumptions identified in Section 3.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 7: Security Objectives for the Environment identifies the security objectives for the environment.

Table 7: Security Objectives for the Environment

Name	TOE Security Objective
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information and the authentication credentials.
OE.AUDIT_REVIEW	The IT Environment will provide the capability to selectively view audit information.
OE.CRYPTANALYTIC	Cryptographic methods used in the TOE shall be independently evaluated to be FIPS 140-1/2 compliant and will be shown to be resistant to cryptanalytic attacks (i.e. will be of adequate strength to protect unclassified Mission Support, Administrative, or Mission Critical data).
OE.MANAGE	The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
OE.NO_EVIL	Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.

Name	TOE Security Objective
OE.PHYSICAL	The IT environment provides physical security, commensurate with the value of the TOE and the data it contains.
OE.PROTECT_MGMT_COMMS	The environment shall protect the transport of audit records to the audit server, remote network management, and authentication server communications with the TOE in a manner that is commensurate with the risks posed to the network.
OE.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.

5. IT Security Requirements

This section provides functional and assurance requirements that must be satisfied by a PP-compliant TOE. These requirements consist of functional components from Part 2 of the Common Criteria (CC) and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section provides information related to the TOE's Security Functional Requirements (SFR). The first subsection addresses strength-of-function (SoF) claims. The second subsection identifies standards compliance methods for the cryptographic SFRs included in this PP. The third subsection specifies the SFRs.

5.1.1 Strength of Function Claims

The statement of the TOE security requirements must include a minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism, except for cryptographic functions. For this PP, the minimum level will be SoF-basic.

In the event that a probabilistic mechanism, such as a password mechanism for user and/or administrator authentication is used, then the expectation is that for each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in a million.

5.1.2 Identification of Standards Compliance Methods

For this PP, cryptographic operations and key management functions must meet FIPS 140-1/2 (Level 1). The methodology used to show compliance to FIPS 140-1/2 standards shall provide proof that the compliance has been certified by a FIPS approved compliance process.

5.2 TOE Security Functional Requirements

The SFRs for the TOE consist of the following components from Part 2 of the CC, summarized in Table 8: TOE Security Functional Requirements. All dependencies among the SFRs are satisfied by the inclusion of the relevant requirement within the TOE security requirements.[6]

[6] FMT_MSA.2 has a dependency on ADV_SPM.1. Section 6 provides the rationale for not including ADV_SPM.1.

Table 8: TOE Security Functional Requirements

Functional Component		Dependencies
FAU_GEN.1-NIAP-0410	Audit data generation	FPT_STM.1
FAU_GEN.2-NIAP-0410	User identity association	FAU_GEN.1 FIA_UID.1
FAU_SEL.1-NIAP-0407	Selective audit	FAU_GEN.1; FMT_MTD.1
FCS_BCM_EXP.1	Explicit: Baseline Cryptographic Module	None
FCS_CKM.1	Cryptographic key generation	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2
FCS_CKM_EXP.2	Cryptographic key establishment	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2
FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1 FMT_MSA.2
FCS_COP_EXP.1	Explicit: Random Number Generation	[FDP_ITC.1or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FCS_COP_EXP.2	Explicit: Cryptographic Operation	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2
FDP_IFC.1 (1)	Subset information flow control (Specified Users Policy)	FDP_IFF.1
FDP_IFC.1 (2)	Subset information flow control (Wireless Encryption Policy)	FDP_IFF.1
FDP_IFF.1-NIAP-0407(1)	Simple security attributes (Specified Client Policy)	FDP_IFC.1 FMT_MSA.3
FDP_IFF.1-NIAP-0407(2)	Simple security attributes (Wireless Encryption Policy)	FDP_IFC.1 FMT_MSA.3
FDP_RIP.1	Subset residual information protection	None
FIA_AFL.1-NIAP-0425(1)	Administrator Authentication failure handling	FIA_UAU.1
FIA_AFL.1-NIAP-0425(2)	User failure handling	FIA_UAU.1
FIA_ATD.1	User attribute definition	None
FIA_UAU.1	Timing of authentication	FIA_UID.1
FIA_UID.1	Timing of identification	None
FIA_USB.1-NIAP-0415	User-subject binding	FIA_ATD.1

Functional Component		Dependencies
FMT_MOF.1(1)	Management of security functions behavior (Cryptographic Function)	FMT_SMR.1
FMT_MOF.1(2)	Management of security functions behavior (Audit Record Generation)	FMT_SMR.1
FMT_MSA.1	Management of security attributes	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1
FMT_MSA.2	Secure security attributes	ADV_SPM.1 [FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1
FMT_MSA.3-NIAP-0409	Static Attribute Initialization (Authorized Users List)	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	Management of TSF data	FMT_SMR.1
FMT_REV.1	Revocation	FMT_SMR.1
FMT_SMF.1(1)	Specification of Management Functions (Cryptographic Function)	None
FMT_SMF.1(2)	Specification of Management Functions (Audit Record Generation)	None
FMT_SMF.1(3)	Specification of Management Functions (Authorized WLAN User List)	None
FMT_SMF.1(4)	Management of TSF data (Cryptographic Key Data)	None
FMT_SMR.1	Security roles	FIA_UID.1
FPT_RVM.1	Non-bypassability of the TOE Security Policy (TSP)	None
FPT_SEP.1	TSF domain separation	None
FPT_STM_EXP.1	Reliable time stamps	None
FPT_TST_EXP.1	TSF Testing	FPT_AMT.1
FPT_TST_EXP.2	TSF Testing of Cryptographic Modules	FPT_AMT.1
FTA_SSL.3	TSF-initiated termination	None
FTA_TAB.1	Default TOE access banners	None

5.2.1.1 FAU_GEN.1-NIAP-0410 Audit data generation

FAU_GEN.1.1-NIAP-0410 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events listed in Table 9;

Table 9: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SEL.1-NIAP-0407	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the Security Administrator performing the function
FCS_CKM_EXP.2	Error(s) detected during cryptographic key transfer	If available - the authentication credentials of subjects with which the invalid key is shared.
FCS_CKM.4	Destruction of a cryptographic key	If available - the authentication credentials of subjects that share the destroyed key.
FDP_IFC.1(1)	Dropping a packet that fails to satisfy the Specified Users Policy	Authentication credentials of source and destination devices
FDP_IFC.1(2)	Dropping a packet that fails to satisfy the Wireless Encryption Policy	Authentication credentials of source and destination devices
FDP_IFF.1-NIAP-0417	Decisions to permit requested information flows	None
FIA_AFL.1-NIAP-	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal	None
FIA_UAU.1	Unsuccessful use of the authentication mechanism	None
FIA_UID.1	Unsuccessful use of the user identification mechanism, including the user identity provided	None
FIA_USB.1-NIAP-0415	Unsuccessful binding of user security attributes to a subject	None
FMT_MOF.1(1)	Changing the TOE encryption algorithm including the selection not to encrypt communications	Encryption algorithm selected (or none)
FMT_MOF.1(2)	Start or Stop of audit record generation	None
FMT_MSA.1	Changing the list of WLAN Devices authorized to communicate with the TOE	User Authentication Credentials added or deleted
FMT_MSA.2	All offered and rejected values for security attributes	None
FMT_MSA.3	Changing the default behavior of the Specified Client Policy	None

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MTD.1(1)	Changing the TOE authentication credentials	Current and previous authentication credentials
FMT_MTD.1(2)	Changes to the cryptographic key data	None – the TOE **SHALL NOT** record cryptographic keys in the audit log.
FMT_REV.1	Unsuccessful revocation of security attributes.	None
FMT_SMR.1	Modifications to the group of users that are part of a role	None
FPT_STM_EXP.1	Changes to the time	None
FPT_TST_EXP.1	Execution of the self test	Success or Failure of test
FPT_TST_EXP.2	Execution of the self test	Success or Failure of test
FTA_SSL.3	TSF Initiated Termination	Termination of an interactive session by the session locking mechanism.

FAU_GEN.1.2-NIAP-0410 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 9].

Application Note: In column 3 of the table below, "if applicable" is used to designate data that should be included in the audit record if it "makes sense" in the context of the event that generates the record. If no other information is required (other than that listed in "a") for a particular audit event type, then an assignment of "none" is acceptable.

5.2.1.2 FAU_GEN.2-NIAP-0410 User identity association

FAU_GEN.2.1-NIAP-0410 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 FAU_SEL.1-NIAP-0407 Selective audit

FAU_SEL.1.1-NIAP-0407 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) *object identity, user identity, subject identity, host identity, event type*

b) *no additional attributes*

5.2.1.4 FCS_BCM_EXP.1 Explicit: Baseline Cryptographic Module

FCS_BCM_EXP.1.1 All cryptomodules shall be FIPS PUB 140-1/2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation.

FCS_BCM_EXP.1.2 The cryptomodule implemented shall have a minimum overall rating of FIPS PUB 140-1/2 Level 1.

Application Note: The term "cryptomodule" has specific meaning and is defined in the terminology section of this Protection Profile.

5.2.1.5 FCS_CKM_EXP.2 Explicit: Cryptographic Key Establishment

FCS_CKM_EXP.2.1 The TSF shall provide the following cryptographic key establishment technique: Cryptographic Key Establishment using Manual Loading
The cryptomodule shall be able to accept as input and be able to output keys in the following circumstances [ST AUTHOR Assignment: circumstances under which the cryptomodule will output a key] in accordance with a specified manual cryptographic key distribution method using FIPS-approved Key Management techniques that meets the FIPS 140-1/2 Key Management Security Levels 1, Key Entry and Output.

Application Note: The ST author should use the assignment to detail the conditions under which key is output from the cryptomodule (for example, only during a certain type of key generation activity).

Note that this requirement mandates that cryptomodules in the TSF have the ability to perform manual key input/output, and that this capability has been through the FIPS validation process. This does not preclude the ST author from specifying additional key establishment techniques.

5.2.1.6 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a [cryptographic key zeroization method] that meets the following:[

a) The Key Zeroization Requirements in FIPS PUB 140-1/2 Key Management Security Levels 1;
b) Zeroization of all private cryptographic keys, plaintext cryptographic keys, key data, and all other critical cryptographic security parameters shall be immediate and complete; and

c) The zeroization shall be executed by overwriting the key/critical cryptographic security parameter storage area three or more times with an alternating pattern.
d) The TSF shall overwrite each intermediate storage area for private cryptographic keys, plaintext cryptographic keys, and all other critical security parameters three or more times with an alternating pattern upon the transfer of the key/CSPs to another location.]

Application Note: Item (d) applies to locations that are used when the keys/parameters are copied during processing, and not to the locations that are used for storage of the keys, which are specified in items (b) and (c). The temporary locations could include memory registers, physical memory locations, and even page files and memory dumps. Configuring the key data may include: setting key lifetimes, setting key length, etc.

5.2.1.7 FCS_COP_EXP.1 Explicit: Random Number Generation

FCS_COP_EXP.1.1 The TSF shall perform all Random Number Generation used by the cryptographic functionality of the TSF using a FIPS-approved Random Number Generator implemented in a FIPS-approved cryptomodule running in a FIPS-approved mode.

Application Note: Whenever a referenced standard calls for a random number generation capability, this requirement specifies the subset of random number generators (those that are FIPS-validated) that are acceptable. Note that the RNG does not have to be implemented in the cryptomodule that is performing the cryptographic operation. Also note that this requirement is not calling for the RNG functionality to be made generally available (e.g., to untrusted users via an API).

5.2.1.8 FCS_COP_EXP.2 Explicit: Cryptographic Operation

FCS_COP_EXP.2.1 A cryptomodule shall perform encryption and decryption using a FIPS-140-1/2 Approved algorithm operating in one or more FIPS 140-1/2 supporting minimum FIPS approved key sizes.

Application Note: The ST author should specify the algorithm used and iterate this requirement for each different algorithm. For example if AES is used the ST author should specify the operation in one or more of ECB, CBC, OFB, CFB1, CFB8, CFB128, or CTR modes supporting key sizes of 128 bits, 192 bits, or 256 bits.

5.2.1.9 FDP_IFC.1(1) Subset information flow control (Specified Users Policy)

FDP_IFC.1.1(1) The TSF shall enforce the [Specified Users SFP] on [subjects: access system; information: network packets; operations: receive packet and transmit packet].

5.2.1.10 FDP_IFC.1(2) Subset information flow control (Wireless Encryption Policy)

FDP_IFC.1.1(2) The TSF shall enforce the [Wireless Encryption SFP] on: [subject: wireless access system; information: network packets and encryption/decryption flag; and operations: encrypt network packets, decrypt network packets].

5.2.1.11 FDP_IFF.1-NIAP-0407(1) Simple Security Attributes (Specified Users Policy)

FDP_IFF.1.1-NIAP-0407(1) The TSF shall enforce the [Specified Users Policy] based on the following types of subject and information security attributes: [authentication credentials].

FDP_IFF.1.2-NIAP-0407(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- The subject is an access system, the operation is transmit packet, and the authentication credentials of the user is allowed based upon the authentication credentials specified in the authentication server;
- The subject is an access system, the operation is receive packet, and auditing events are allowed based upon the administrator specified list of authentication credentials;
- [ST AUTHOR - selection: [ST AUTHOR - assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes], “no additional information flow Specified Users Policy Rules”].

FDP_IFF.1.3-NIAP-0407(1) The TSF shall enforce the following information flow control rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: additional information flow control SFP rules], "no additional information flow control SFP rules"].

FDP_IFF.1.4-NIAP-0407(1) The TSF shall provide the following [ST AUTHOR - selection: [ST AUTHOR - assignment: list of additional SFP capabilities], "no additional SFP capabilities"].

FDP_IFF.1.5-NIAP-0407(1) The TSF shall explicitly authorize an information flow based on the following rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: rules, based on security attributes, that explicitly authorize information flows], "no explicit authorization rules"].

FDP_IFF.1.6-NIAP-0407(1) The TSF shall explicitly deny an information flow based on the following rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: rules, based on security attributes, that explicitly deny information flows], "no explicit denial rules"].

Application Note: The ST Author should use the selections and assignments in elements 1.2 thru 1.5 to indicate exceptions to the Specified Users Policy (e.g. broadcast packets).

5.2.1.12 FDP_IFF.1-NIAP-0407(2) Simple Security Attributes (Wireless Encryption Policy)

FDP_IFF.1.1-NIAP-0407(2) The TSF shall enforce the [Wireless Encryption Policy] based on the following types of subject and information security attributes: [encryption/decryption flag; subject type].

FDP_IFF.1.2-NIAP-0407(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the encryption/decryption flag does NOT indicate that the TOE should perform encryption then all packets may pass without modification.
- If the subject type is wireless access system, the operation is transmit the network packet, and the encryption/decryption flag indicates the TOE should perform encryption, then the TOE must encrypt user data via FCS_COP_EXP.2.1 to permit the information flow.
- If the subject type is wireless access system, the operation is pass the network packet, and the encryption/decryption flag indicates the TOE should perform encryption then the TOE must decrypt user data via FCS_COP_EXP.2.1 to permit the information flow.
- [ST AUTHOR - selection: [ST AUTHOR - assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes], “no additional information flow Specified Users Policy Rules”].

FDP_IFF.1.3-NIAP-0407(2) The TSF shall enforce the following information flow control rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: additional information flow control SFP rules], "no additional information flow control SFP rules"].

FDP_IFF.1.4-NIAP-0407(2) The TSF shall provide the following [ST AUTHOR - selection: [ST AUTHOR - assignment: list of additional SFP capabilities], "no additional SFP capabilities"].

FDP_IFF.1.5-NIAP-0407(2) The TSF shall explicitly authorize an information flow based on the following rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: rules, based on security attributes, that explicitly authorize information flows], "no explicit authorization rules"].

FDP_IFF.1.6-NIAP-0407(2) The TSF shall explicitly deny an information flow based on the following rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: rules, based on security attributes, that explicitly deny information flows], "no explicit denial rules"].

Application Note: For FDP_IFF.1.2-NIAP-0407(2) the operations "transmit" and "pass" are specific to the type of medium over which the network packets are transmitted. The operation "transmit" applies to the network packets that are sent out over the wireless side of the network. The information is broadcast over the air, therefore the TOE must perform encryption. The operation "pass" is specific for the wired side of the network, therefore the TOE must perform decryption but it is not required to perform encryption to allow the information to flow through the wired side of the network because the wired side is assumed to be a trusted network.

Application Note: The ST Author should use the selections and assignments in elements 1.2 thru 1.5 to indicate exceptions to the Wireless Encryption Policy (e.g. broadcast/management packets).

5.2.1.13 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [vendor specified components of the wireless access system].

5.2.1.14 FIA_AFL.1-NIAP-0425(1) Administrator Authentication failure handling

FIA_AFL.1.1-NIAP-0425 The TSF shall detect when **an authorized administrator configurable integer of** unsuccessful authentication attempts occur related to [remote administrators logging on to the WLAN access system].

Application note: This requirement applies to remote administrators and does not apply to the local administration of the TOE, since it does not make sense to lock a local administrator's account in this fashion. For the purpose of this PP, 'local' refers to the administrator who has physical access to the TOE.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the administrator from performing activities remotely that require authentication until an action is taken by a local Administrator].

5.2.1.15 FIA_AFL.1-NIAP-0425(2) User Authentication failure handling

FIA_AFL.1.1-NIAP-0425 The TSF shall detect when **an authorized user configurable integer of** unsuccessful authentication attempts occur related to [remote users logging on to the WLAN access system].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the user from performing activities remotely that require authentication until an action is taken by a local Administrator].

5.2.1.16 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following **minimum** list of security attributes belonging to individual users: [Authentication Credentials].

Application Note: Authentication Credentials may include user ID, passwords, digital certificates, etc.

5.2.1.17 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [the passing of network traffic through the access system, the passing of authentication data to and from the authentication server, the passing of audit events to the audit log] on behalf of the user to be performed before the user is authenticated.

Application Note: In this requirement network traffic applies to the non-user specific information that must be allowed to pass before authentication. Management and control packets are allowed to pass before authentication. For example, the information conveyed in management frames is used for various link-layer maintenance functions.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.1.18 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [the passing of network traffic through the access system, the passing of authentication data to and from the authentication server, the passing of audit events to the audit log] on behalf of the user to be performed the user is identified.

FIA_UID.1.2 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.1.19 FIA_USB.1-NIAP-0415 User-subject binding

FIA_USB.1.1 –NIAP-0415 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [authentication credentials].

5.2.1.20 FMT_MOF.1(1) Management of security functions behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to *modify the behavior* of the **cryptographic** functions [access system configuration, maximum number of unsuccessful remote authentication attempts, and maximum time intervals of remote user inactivity] to [the authorized administrator].

5.2.1.21 FMT_MOF.1(2) Management of security functions behavior

FMT_MOF.1.1 (2) The TSF shall restrict the ability to *enable, disable, determine, and modify the behavior* of the **audit record generation** functions [access system configuration, maximum number of unsuccessful remote authentication attempts, and maximum time intervals of remote user inactivity] to [the authorized administrator].

5.2.1.22 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Wireless Encryption SFP] to restrict the ability to *modify* the value of the object security attributes to [authorized administrators and owners of the object].

5.2.1.23 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.2.1.24 FMT_MSA.3-NIAP-0409 Static Attribute Initialization (Authorized User List)

FMT_MSA.3.1-NIAP-0409 The TSF shall enforce the [Specified Users Policy] to provide [ST AUTHOR – selection: restrictive, permissive, [other property]] default values of [ST _AUTHOR assignment: the value that is initially set] for the information flow policy attributes used to enforce the SFP.

Application Note: The ST author should characterize the default state and indicate the default values associated with the WLAN System.

Application Note: The term "Authorized WLAN User List" is synonymous with "the database of authentication credentials with which the TOE may communicate over the RF communications channel".

FMT_MSA.3.2-NIAP-0409 The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.2.1.25 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query, modify, delete, clear,* **and create** the **security relevant TSF data except for audit records, user security attributes, and critical security parameters** to [the authorized administrator].

Application Note: The restrictions for audit records, user security attributes and critical security parameters are specified below.

FMT_MTD.1.1(2) The TSF shall restrict the ability to **initialize** [the authentication data] to [authorized administrators and authorized users].

FMT_MTD.1.1(3) The TSF shall restrict the ability to **initialize and modify** [the critical security parameters] to [administrators].

5.2.1.26 FMT_REV.1 Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the *users* within the TSC to [the authorized administrator].

FMT_REV.1.2 The TSF shall enforce the rules [for validation of authentication credentials].

5.2.1.27 FMT_SMF.1(1) Specification of Management Functions[7] (Cryptographic Function)

FMT_SMF.1.1(1) The TSF shall be capable of performing the following management functions: [query and set the encryption/decryption of network packets (FCS_COP.EXP.1), or query and set no encryption/decryption of network packets].

Application Note: This requirement ensures that those responsible for TOE administration are able to select an encryption algorithm identified in FCS_COP.EXP.1 or no encryption for encrypting/decrypting data transmitted by the over the wireless communications channel.

5.2.1.28 FMT_SMF.1(2) Specification of Management Functions (TOE Audit Record Generation)

FMT_SMF.1.1(2) The TSF shall be capable of performing the following management functions: [query, enable or disable Security Audit (FAU_GEN.1-NIAP-0410)].

Application Note: This requirement ensures that those responsible for TOE administration are able to start or stop the TOE generation of audit records

[7] The FMT_SMF (Specification of Management Functions) family is documented in CCIMB interpretation 65.

5.2.1.29 FMT_SMF.1(3) Specification of Management Functions (Authorized User List)

FMT_SMF.1.1(3) The TSF shall be capable of performing the following management functions: [The TSF shall support the Specified Users Policy by providing the ability to query, modify, and delete entries in the database of authentication credentials in the authentication server with which the TOE may communicate].

Application Note: This requirement ensures those responsible for TOE administration are able to set the authentication credentials of one or more users that are permitted to communicate with or through the TOE via the RF communications channel.

Application Note: The term "Authorized User List" is synonymous with "the database of authentication credentials of which the TOE may communicate" over the RF communications channel.

5.2.1.30 FMT_SMF.1(4) Specification of Management Functions (Cryptographic Key Data)

FMT_SMF.1.1(4) The TSF shall be capable of performing the following management functions: [query, set, modify, and delete the cryptographic keys and key data in support of the Wireless Encryption Policy].

Application Note: The intent of this requirement is to provide the ability to configure the TOE's cryptographic key(s). Configuring the key data may include: setting key lifetimes, setting key length, etc.

5.2.1.31 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [the authorized administrator].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.1.32 FPT_RVM.1 Non-bypassability of the TOE Security Policy (TSP)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.1.33 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2.1.34 FPT_STM_EXP.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to **obtain** reliable time stamps for its own use.

5.2.1.35 FPT_TST_EXP.1 TSF Testing

FPT_TST_EXP.1.1 The TSF shall run a suite of self-tests during initial start-up and upon request, to demonstrate the correct operation of the hardware portions of the TSF.

FPT_TST_EXP.1.2 The TSF shall provide the capability to use a TSF-provided cryptographic function to verify the integrity of all TSF data except the following: audit data, [ST AUTHOR -selection: [ST AUTHOR - assignment: *other dynamic TSF data for which no integrity validation is justified*], *none*].

FPT_TST_EXP.1.3 The TSF shall provide the capability to use a TSF-provided cryptographic function to verify the integrity of stored TSF executable code.

Application Note: In element 4.1, only the hardware portions of the TSF need to be self-tested; this makes sense because hardware has the capability of degrading or failing over time, while software generally doesn't. TSF software integrity is addressed by element 4.3. In element 4.2, the ST author should specify the TSF data for which integrity validation is not required. While some TSF data are dynamic and therefore not amenable to integrity verification, it is expected that all TSF data for which integrity verification "makes sense" be subject to this requirement.

5.2.1.36 FPT_TST_EXP.2 TSF Testing of Cryptographic Modules

FPT_TST_EXP.2.1 The TSF shall run the suite of self-tests provided by the FIPS 140-1/2 cryptomodule during initial start-up (power on) and upon request, to demonstrate the correct operation of the cryptographic components of the TSF.

FPT_TST_EXP.2.2 The TSF shall be able to run the suite of self-tests provided by the FIPS 140-1/2 cryptomodule immediately after the generation of a key.

Application Note: The 2.2 element requires specific functionality IF the TOE generates cryptographic keys. This element does not require the TOE to generate keys.

5.2.1.37 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive **administrator** session after a [configurable time interval of user inactivity].

5.2.1.38 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

5.3 Security Requirements for the IT Environment

This Protection Profile provides functional requirements for the IT Environment. The IT environment includes the authentication server, the management console, and the audit collection server, and authorized IT entities (e.g., a certificate authority server, NTP server).

Table 10: Security Functional Requirements for the TOE IT Environment

Functional Component		Dependencies[8]
FAU_SAA.1-NIAP-0407	Potential violation analysis	FAU_GEN.1
FAU_SAR.1	Audit review	FAU_GEN.1
FAU_SAR.2	Restricted audit review	FAU_SAR.1
FAU_SAR.3	Selectable audit review	FAU_SAR.1
FAU_STG.1-NIAP-0429	Protected audit trail storage	FAU_GEN.1
FAU_STG.3	Action in case of possible audit data loss	FAU_STG.1
FDP_IFC.2	Complete information flow control	FDP_IFF.1
FDP_IFF.1-NIAP-0427	Simple Security Attributes (Wireless Encryption Policy)	FDP_IFC.1 FMT_MSA.3
FDP_ITT.1	Basic internal transfer protection	FDP_IFC.1
FDP_ITT.3	Integrity monitoring	FDP_IFC.1; FDP_ITT.1
FDP_RIP.1	Subset residual information protection	None
FIA_USB.1-NIAP-0415	User-subject binding	FIA_ATD.1
FMT_MOF.1	Management of security functions behavior	FMT_SMR.1
FMT_SMR.1	Security roles	FIA_UID.1

[8] The purpose of requirements on the IT environment is to supplement the TOE and to ensure that the TOE and the IT environment together satisfy all security objectives. In order to limit the scope of the IT environment only those IT environmental requirements that directly contribute to the satisfaction of objectives have been included in this PP. Requirements for the IT environment necessary simply to satisfy management guidance, audit guidance, or dependency chains have not been included in this PP.

Functional Component		Dependencies[8]
FPT_STM.1	Reliable time stamps	None
FTA_SSL.1	TSF-initiated session locking	FIA_UAU.1
FTA_SSL.2	User-initiated locking	FIA_UAU.1

5.3.1 FAU_SAA.1-NIAP-0407 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP

FAU_SAA.1.2-NIAP-0407 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation **of a single auditable event** or combination of [auditable events in Table 9] known to indicate a potential security violation;

b) *no additional rules*

5.3.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide authorised administrators with the capability to read list of auditable events provided in Table 9 from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.3.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.3.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches, sorting, ordering* of audit data based on [criteria with logical relations].

5.3.5 FAU_STG.1-NIAP-0429 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2- NIAP-0429 The TSF shall be able to *prevent* modifications to the audit records in the audit trail.

5.3.6 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall [immediately alert the administrators by displaying a message at the local console, [selection:[assignment: other actions determined by the ST author], "none"]] if the audit trail exceeds [an Administrator-settable percentage of storage capacity].

Application Note: The ST Author should determine if there are other actions that should be taken when the audit trial setting is exceeded, and put these in the assignment. If there are no other actions, then the ST Author should select "none".

5.3.7 FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the [Specified Users SFP] on [wireless access system] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

5.3.8 FDP_IFF.1-NIAP-0407(2) Simple Security Attributes (Wireless Encryption Policy)

FDP_IFF.1.1-NIAP-0407(2) The TSF shall enforce the [Wireless Encryption Policy] based on the following types of subject and information security attributes: [encryption/decryption flag; subject type].

FDP_IFF.1.2-NIAP-0407(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the encryption/decryption flag does NOT indicate that the TOE should perform encryption then all packets may pass without modification.
- If the subject type is wireless access system, the operation is transmit the network packet, and the encryption/decryption flag indicates the TOE should perform encryption, then the TOE

must encrypt user data via FCS_COP_EXP.2.1 to permit the information flow.

- If the subject type is wireless access system, the operation is pass the network packet, and the encryption/decryption flag indicates the TOE should perform encryption then the TOE must decrypt user data via FCS_COP_EXP.2.1 to permit the information flow.
- [ST AUTHOR - selection: [ST AUTHOR - assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes], “no additional information flow Specified Users Policy Rules”].

FDP_IFF.1.3-NIAP-0407(2) The TSF shall enforce the following information flow control rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: additional information flow control SFP rules], "no additional information flow control SFP rules"].

FDP_IFF.1.4-NIAP-0407(2) The TSF shall provide the following [ST AUTHOR - selection: [ST AUTHOR - assignment: list of additional SFP capabilities], "no additional SFP capabilities"].

FDP_IFF.1.5-NIAP-0407(2) The TSF shall explicitly authorize an information flow based on the following rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: rules, based on security attributes, that explicitly authorize information flows], "no explicit authorization rules"].

FDP_IFF.1.6-NIAP-0407(2) The TSF shall explicitly deny an information flow based on the following rules: [ST AUTHOR - selection: [ST AUTHOR - assignment: rules, based on security attributes, that explicitly deny information flows], "no explicit denial rules"].

Application Note: The ST Author should use the selections and assignments in elements 1.2 thru 1.5 to indicate exceptions to the Wireless Encryption Policy (e.g. broadcast/management packets).

5.3.9 FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the [Wireless Encryption SFP and/or Specified Users SFP] to prevent the *disclosure, modification, loss of use of user data* when it is transmitted between physically-separated parts of the TOE.

5.3.10 FDP_ITT.3 Integrity monitoring

FDP_ITT.3.1 The TSF shall enforce the [Specified Users SFP] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [integrity errors].

FCP_ITT.3.2 Upon detection of a data integrity error, the TSF shall [inform authorized administrator].

5.3.11 FDP_RIP.1 Subset residual information protection

FDP_RIP.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [vendor specified components of the wireless access system].

5.3.12 FIA_USB.1-NIAP-0415 User-subject binding

FIA_USB.1.1-NIAP-0415 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [authentication credentials].

5.3.13 FMT_MOF.1(1) Management of security functions behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to *modify the behavior* of the **cryptographic** functions [access system configuration, maximum number of unsuccessful remote authentication attempts, and maximum time intervals of remote user inactivity] to [the authorized administrator].

5.3.14 FMT_MOF.1(2) Management of security functions behavior

FMT_MOF.1.1 (2) The TSF shall restrict the ability to *enable, disable, determine, and modify the behavior* of the **audit record generation** functions [access system configuration, maximum number of unsuccessful remote authentication attempts, and maximum time intervals of remote user inactivity] to [the authorized administrator].

5.3.15 FPT_STM_EXP.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to obtain reliable time stamps for its own use.

5.3.16 FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after a system administrator configurable time of user inactivity by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [none].

5.3.17 FTA_SSL.2 User-initiated locking

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session, by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [none].

5.4 TOE Security Assurance Requirements

The TOE security assurance requirements summarized in Table 11: TOE Assurance Requirements, identify the management and evaluative activities required to address the threats and policies identified in section 3 of this protection profile. Section 5 provides a justification for the chosen security assurance requirements and the selected assurance level EAL2 augmented with, ACM_SCP.1 (CM Coverage), ALC_FLR.2 (Flaw Remediation), and AVA_MSU.1 (Misuse – Examination of guidance).

Table 11: TOE Assurance Requirements

Assurance Class	Assurance Components
Configuration Management	Authorization controls (ACM_CAP.3) as modified by NIAP Interpretation I-0412) TOE CM Coverage (ACM_SCP.1)
Delivery and Operations	Delivery procedures (ADO_DEL.1) Installation, generation, and start-up procedures (ADO_IGS.1)
Development	Informal functional specification (ADV_FSP.1) Security enforcing high-level design (ADV_HLD.1) Informal correspondence demonstration (ADV_RCR.1)
Guidance documents	Administrator guidance (AGD_ADM.1) User guidance (AGD_USR.1)
Life-Cycle Support	Flaw Reporting Procedures (ALC_FLR.2)

Assurance Class	Assurance Components
Tests	Analysis of coverage (ATE_COV.1) Functional testing (ATE_FUN.1) Independent testing - sample (ATE_IND.2)
Vulnerability Assessment	Examination of guidance (AVA_MSU.1) Strength of TOE security function evaluation (AVA_SOF.1) Developer vulnerability analysis (AVA_VLA.1)

6. Rationale

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined in Section 3 and Section 4, respectively. Additionally, this section describes the rationale for not satisfying all of the dependencies and the rationale for the strength of function (SOF) claim. Table 12 illustrates the mapping from Security Objectives to Threats and Policies.

6.1 Rationale for Security Objectives

Table 12: Security Objectives to Threats and Policies Mappings

Threat/Policy	Objectives Addressing the Threat	Rationale

Threat/Policy	Objectives Addressing the Threat	Rationale
T.ACCIDENTAL_ADMIN_ ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management. O.MANAGE The TOE will provide those functions and facilities necessary to support the administrators in their management of the security of the TOE. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. OE.NO_EVIL Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.	O.ADMIN_GUIDANCE (ADO_DEL.2, ADO_IGS.1, AGD_ADM.1, AGD_USR.1, AVA_MSU.2) help to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure. O.MANAGE (FMT_MTD.1.1(1)(2)(3)) also contributes to mitigating this threat by providing administrators the capability to view configuration settings. For example, if the Security Administrator made a mistake when configuring the set of permitted users authentication credentials, providing them the capability to view the lists of authentication credentials affords them the ability to review the list and discover any mistakes that might have been made. OE.MANAGE (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3) ensures that the administrator can view security relevant audit events.
T.ACCIDENTAL_CRYPTO_C OMPROMISE A user or process may cause key data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. O.SELF_PROTECTION The TOE will maintain a domain for itself and the TOE's own execution that protects them and their resources from external interference, tampering, or unauthorized disclosure through their interfaces.	O.RESIDUAL_INFORMATION; OE.RESIDUAL_INFORMATION (FDP_RIP.1, FCS_CKM_EXP.2, FCS_CKM.4) contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION (FPT_SEP.1 and FPT_RVM.1) ensure that the TOE will have adequate protection from external sources and that all TSP functions are invoked.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.MASQUERADE A user may masquerade as an authorized user or the authentication server to gain access to data or TOE resources.	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS (FIA_AFL.1-NIAP-0425(1), FIA_ATD.1, FIA_UID.1, FIA_UAU.1, AVA_SOF.1) mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T.POOR_DESIGN Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly. O.DOCUMENTED_ DESIGN The design of the TOE is adequately and accurately documented. O.VULNERABILITY_ ANALYSIS The TOE will undergo vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATION (ACM_CAP.2, ACM_SCP.1, ALC_FLR.2) plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design documentation and the ability to report and resolve security flaws. O.DOCUMENTED_DESIGN (ADV_FSP.1, ADV_HLD.1, ADV_RCR.1) counters this threat, to a degree, by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_RCR.1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification. O.VULNERABILITY_ANALYSIS_TEST (AVA_VLA.1) ensure that the TOE has been analyzed for obvious vulnerabilities and that any vulnerabilities found have been removed or otherwise mitigated, this includes analysis of any probabilistic or permutational mechanisms incorporated into a TOE claiming conformance to this PP.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.POOR_IMPLEMENTATION Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly. O.PARTIAL_FUNCTIONAL_TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ ANALYSIS The TOE will undergo vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATION (ACM_CAP.2, ACM_SCP.1, ALC_FLR.2) plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. This ensures that changes to the TOE are performed in structure manner and tracked. O.PARTIAL_FUNCTIONAL_TESTING (ATE_COV.1, ATE_FUN.1, ATE_IND.2) ATE_COV.1 ensures that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing. O.VULNERABILITY_ANALYSIS_TEST (AVA_VLA.1) ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.
T.POOR_TEST Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.	O.CORRECT_ TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. O.PARTIAL_FUNCTIONAL_TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.PARTIAL_FUNCTIONAL_TESTING (ATE_COV.1, ATE_FUN.1, ATE_IND.2) ATE_COV.1 ensures that the developers provide evidence and demonstration that all security functions perform as specified through independent sample testing. O.CORRECT_ TSF_OPERATION (FPT_TST_EXP.1(1), FPT_TST_EXP.1(2), FPT_TST_EXP.1(3)) ensure that users can verify the continued correct operation of the TOE after it has been installed in its target environment. O.VULNERABILITY_ANALYSIS_TEST (AVA_VLA.1) ensures that the TOE has been analyzed and tested to demonstrate that it is resistant to obvious vulnerabilities.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION; OE.RESIDUAL_INFORMATION (FDP_RIP.1, FCS_CKM_EXP.2, FCS_CKM.4) contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed.
T.TSF_COMPROMISE A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).	O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. O.SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its interfaces.	O.MANAGE (FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.2, FMT_MSA.3-NIAP-0409, FMT_MTD.1.1(1)(2)(3)) mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. OE.MANAGE (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3) ensures that the administrator can view security relevant audit events. O.RESIDUAL_INFORMATION (FDP_RIP.1, FCS_CKM_EXP.2, FCS_CKM.4)) and OE.RESIDUAL_INFORMATION (FDP_RIP.1(IT 2)) contributes to the mitigation of this threat by ensuring that any residual data is removed from network packet objects and ensuing that cryptographic material is not accessible once it is no longer needed. O.SELF_PROTECTION (FPT_SEP.1, FPT_RVM.1) requires that the TOE environment be able to protect itself from tampering and that the security mechanisms in the TOE cannot be bypassed. Without this objective, there could be no assurance that users could not view or modify TSF data or TSF executables.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session.	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	The only sessions that are established with the TOE are anticipated to be administrative sessions. Hence, this threat is restricted to administrative sessions. The termination of general user sessions is expected to be handled by the IT environment. O.TOE_ACCESS (FTA_SSL.3) helps to mitigate this threat by including mechanisms that place controls on administrator sessions. Administrator sessions are dropped after a Security Administrator defined time period of inactivity. Dropping the connection of a session (after the specified time period) reduces the risk of someone accessing the machine where the session was established, thus gaining unauthorized access to the session.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.UNAUTHORIZED_ACCESS A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.	O.MEDIATE The TOE must mediate the flow of information to and from wireless clients communicating via the TOE in accordance with its security policy.	O.MEDIATE (FDP_IFF.1-NIAP-0407(1), FDP_IFF.1-NIAP-0407(2), FDP_IFC.1(1), FDP_IFC.1(2), FMT_REV.1, FPT_RVM.1) works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. One of the rules ensures that the network identifier in a packet is in the set of network identifiers associated with a TOE's network interface. Therefore, if a user supplied a network identifier in a packet that purported to originate from a network associated with a TOE network interface other than the one the user supplied the packet on, the packet would not be allowed to flow through the TOE, or access TOE services. Another rule provides further granularity of access control by enabling the administrator to control the source and destination address, destination port, protocol, and application level commands. By implementing this level of access control an attacker would not be allowed access to other hosts and applications residing on the protected network. Additionally, the TOE maintains "state" information of all approved connections. This function ensures that each packet arriving at a TOE interface purporting to be part of an approved connection through or to the TOE, is checked against a current and valid list of connection parameters (e.g. for a TCP/IP connection; source and destination address, ports, SYN and ACK numbers, flags, etc.) prior to allowing the packet through or to the TOE. The TOE requires successful authentication (strong authentication via single-use password, encrypted authentication and/or both, with account lock-out capability) to the TOE prior to gaining access to certain services on or mediated by the TOE. By implementing strong authentication to gain access to these services, an attacker's opportunity to successfully conduct a man-in-the-middle and/or password guessing attack is greatly reduced. Lastly, the TSF must ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc to the Security Administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.UNAUTH_ADMIN_ACCESS An unauthorized user or process may gain access to an administrative account.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management. O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE. OE.NO_EVIL Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.	O.ADMIN_GUIDANCE (ADO_DEL.2, ADO_IGS.1, AGD_ADM.1, AGD_USR.1, AVA_MSU.2) help to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure. O.MANAGE (FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.2, FMT_MSA.3-NIAP-0409, FMT_MTD.1.1(1)(2)(3)) mitigate this threat by restricting access to administrative functions and management of TSF data to the administrator. O.TOE_ACCESS (FTA_SSL.3) helps to mitigate this threat by including mechanisms that place controls on administrator sessions. OE.NO_EVIL (AGD_ADM) help to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.

Threat/Policy	Objectives Addressing the Threat	Rationale
T.UNIDENTIFIED_ACTIONS The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	OE.AUDIT_REVIEW The TOE will provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.	O.AUDIT_REVIEW (FAU_SAA.1-NIAP-0407, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3) helps to mitigate this threat by providing the Security Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events (e.g. set number of authentication failures, set number of information policy flow failures, self-test failures, etc.) and immediately notifies all TOE administrators once an event has occurred or a set threshold has been met. If a potential security violation has been detected, the TOE displays a message that identifies the potential security violation to all administrative consoles. The consoles include the local TOE console and any active remote administrative sessions. If an administrator is not currently logged into the TOE, the message is stored and immediately displayed the next time an administrator logs into the TOE. This message is displayed to all administrative roles and will remain on the screen for each administrative role until each administrative role acknowledges the message. In addition to displaying the potential security violation, the message must contain all audit records that generated the potential security violation. By enforcing the message content and display, this objective provides assurance that a TOE administrator will be notified of a potential security violation. The TOE also requires an Audit Administrative role. This role is restricted to Audit record review only. A search and sort capability provides an efficient mechanism for the Audit Administrator to view pertinent audit information.
P.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	O.DISPLAY_BANNER (FTA_TAB.1) satisfies this policy by ensuring that the TOE displays a Security Administrator configurable banner that provides all users with a warning about the unauthorized use of the TOE. A banner will be presented for all TOE services that require authentication. In other words, it will be required for all administrative actions. The presentation of banners prior to actions that take place in the environment as a result of the passing of traffic through the TOE is assumed to be provided by the IT environment.

Threat/Policy	Objectives Addressing the Threat	Rationale
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events. O.MANAGE The TOE will provide functions and facilities necessary to support the administrators in their management of the security of the TOE., and restrict these functions and facilities from unauthorized use. OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. O.TIME_STAMPS The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.AUDIT_GENERATION (FAU_GEN.1-NIAP-0410, FAU_GEN.2-NIAP-0410, FAU_SEL.1-NIAP-0407, FIA_USB.1-NIAP-0415) addresses this policy by providing the Security Administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.). O.MANAGE (FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.2, FMT_MSA.3-NIAP-0409, FMT_MTD.1.1(1)(2)(3)) ensure that access to administrative functions and management of TSF data is restricted to the administrator. OE.MANAGE (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3) ensure that the administrator can review the audit event log restricts access to this information to the administrator O.TIME_STAMPS (FPT_STM.1, FMT_MTD.1(3)) plays a role in supporting this policy by requiring the TOE to provide a reliable time stamp (configured locally by the Security Administrator or via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred. O.TOE_ACCESS (FIA_AFL.1-NIAP-0425(1), FIA_ATD.1, FIA_UID.1, FIA_UAU.1, , AVA_SOF.1) supports this policy by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.

Threat/Policy	Objectives Addressing the Threat	Rationale
P.CRYPTOGRAPHY Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).	O.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-1/2 validated cryptographic services.	O.CRYPTOGRAPHY (FCS_BCM_EXP.1, FCS_CKM_EXP.2, FCS_CKM.4, FCS_COP_EXP.1) satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE. O.RESIDUAL_INFORMATION (FCS_CKM_EXP.2, FCS_CKM.4) satisfies this policy by ensuring that cryptographic data are cleared according to FIPS 140-1/2.
P.ENCRYPTED_CHANNEL The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.	O.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-1/2 validated cryptographic services. OE.CRYPTANALYTIC Cryptographic methods used in the TOE shall be independently evaluated to be FIPS 140-1/2compliant and will be shown to be resistant to cryptanalytic attacks (i.e. will be of adequate strength to protect unclassified Mission Support, Administrative, or Mission Critical data).	O.CRYPTOGRAPHY OE.CRYPTANALYTIC (FCS_BCM_EXP.1, FCS_CKM.2, FCS_CKM.4, FCS_CKM_EXP.2, FCS_COP_EXP.1) satisfies this policy by requiring the TOE to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity protection of TSF data while in transit to remote parts of the TOE.

Threat/Policy	Objectives Addressing the Threat	Rationale
P.NO_AD_HOC_NETWORKS In concordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.	O.MEDIATE	O.MEDIATE (FDP_IFF.1-NIAP-0407(1), FDP_IFF.1-NIAP-0407(2), FDP_IFC.1(1), FDP_IFC.1(2), FMT_REV.1, FPT_RVM.1) works to mitigate this threat by ensuring that all network packets that flow through the TOE are subject to the information flow policies. One of the rules ensures that the network identifier in a packet is in the set of network identifiers associated with a TOE's network interface. Therefore, if a user supplied a network identifier in a packet that purported to originate from a network associated with a TOE network interface other than the one the user supplied the packet on, the packet would not be allowed to flow through the TOE, or access TOE services. Another rule provides further granularity of access control by enabling the administrator to control the source and destination address, destination port, protocol, and application level commands. By implementing this level of access control an attacker would not be allowed access to other hosts and applications residing on the protected network. Additionally, the TOE maintains "state" information of all approved connections. This function ensures that each packet arriving at a TOE interface purporting to be part of an approved connection through or to the TOE, is checked against a current and valid list of connection parameters (e.g. for a TCP/IP connection; source and destination address, ports, SYN and ACK numbers, flags, etc.) prior to allowing the packet through or to the TOE. The TOE requires successful authentication (strong authentication via single-use password, encrypted authentication and/or both, with account lock-out capability) to the TOE prior to gaining access to certain services on or mediated by the TOE. By implementing strong authentication to gain access to these services, an attacker's opportunity to successfully conduct a man-in-the-middle and/or password guessing attack is greatly reduced. Lastly, the TSF must ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc to the Security Administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

6.2 Additional Rationale for Security Objectives in the TOE IT Environment

Three of the security objectives for the TOE are simply restatements of an assumption found in Section 3. Therefore, these three objectives for the environment, OE.BASIC_ROBUSTNESS_OS, OE.NO_EVIL and OE.PHYSICAL, trace to the assumptions trivially.

Of these three, only OE.BASIC_ROBUSTNESS_OS bares further discussion. This assumption has been included in the PP because the TOE is not expected to address all of the threats and policies defined in a basic robustness environment. As such, the eventual user of the TOE must take additional steps to ensure the environment in which the TOE is used, has been hardened to the basic robustness level. This objective and its corresponding assumption should NOT be construed to allow the TOE IT environment to satisfy objectives or requirements levied on the TOE.

The remainder of the security objectives for the IT environment has been included in this Protection Profile in order to support the TOE security functions. The rationale support is documented in Table along with the rationale for security objectives for the TOE.
All of the security objectives are either referenced in the previous section with regards to specific threats or they are direct rephrasing of assumptions.

6.3 Rationale for TOE Security Requirements

Table 13: Rationale for TOE Security Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management.	ADO_DEL.1 ADO_IGS.1 AGD_ADM.1 AGD_USR.1 AVA_MSU.1	ADO_DEL.1 ensures that the administrator has the ability to begin their TOE installation with a *clean* (e.g., malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE The ADO_IGS.1 requirement ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The Installation, Generation and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration. The AGD_ADM.1 requirement mandates the developer provide the administrator with guidance

Objective	Requirements Addressing the Objective	Rationale
		on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a description of how to setup and review the auditing features of the TOE. The AGD_USR.1 is intended for non-administrative users. If the TOE provides facilities/interfaces for this type of user, this guidance will describe how to use those interfaces securely. This could include guidance on the setup of wireless clients for use with the TOE. If it is the case that the wireless clients may be configured by administrators that are not administrators of this TOE, then that guidance may be user guidance from the perspective of this TOE. AVA_MSU.1 ensures that the guidance documentation can be followed unambiguously to ensure the TOE is not mis-configured in an unsecure state due to confusing guidance.
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security-relevant events.	FAU_GEN.1-NIAP-0410 FAU_GEN.2-NIAP-0410 FAU_SEL.1-NIAP-0407 FIA_USB.1-NIAP-0415	FAU_GEN.1-NIAP-0410 defines the set of events that the TOE must be capable of recording. This requirement ensures that the Security Administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this PP. FAU_GEN.2-NIAP-0410 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated. FAU_SEL.1-NIAP-0407allows for the selection of events to be audited. This requires that the criteria used for the selection of auditable events to be defined. For example, the user identity can be used as selection criteria for the events to be auditied. FIA_USB.1-NIAP-0415 plays a role is satisfying this objective by requiring a binding of security attributes

Objective	Requirements Addressing the Objective	Rationale
		associated with users that are authenticated with the subjects that represent them in the TOE. This only applies to authorized users, since the identity of unauthenticated users cannot be confirmed. Therefore, the audit trail may not always have the proper identity of the subject that causes an audit record to be generated (e.g., presumed network address of an unauthenticated user may be a spoofed address).
O.CONFIGURATION_ IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.	ACM_CAP.2 ACM_SCP.1 ALC_FLR.2	ACM_CAP.2 contributes to this objective by requiring the developer have a configuration management plan that describes how changes to the TOE and its evaluation deliverables are managed. ACM_SCP.1 is necessary to define the items that must be under the control of the CM system. This requirement ensures that the TOE implementation representation, design documentation, test documentation (including the executable test suite), user and administrator guidance, and CM documentation are tracked by the CM system. ALC_FLR.2 plays a role in satisfying this objective by requiring the developer to have procedures that address flaws that have been discovered in the product, either through developer actions (e.g., developer testing) or those discovered by others. The flaw remediation process used by the developer corrects any discovered flaws and performs an analysis to ensure new flaws are not created while fixing the discovered flaws.
O.CORRECT_ TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FPT_TST_EXP.1 FPT_TST_EXP.2	FPT_TST_EXP.1 is necessary to ensure the correct operation TSF hardware. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupt the TOE may not correctly enforce its security policies. The FPT_TST_EXP.2 functional addresses the critical nature and specific handling of the cryptographic related TSF data. Since the cryptographic TSF data has specific FIPS PUB requirements associated with them it is important to ensure that any fielded testing on the integrity of these data maintains the same level of scrutiny as specified in the FCS functional requirements.
O.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-1/2 validated cryptographic services.	FCS_BCM_EXP.1 FCS_CKM_EXP.2 FCS_CKM.4 FCS_COP_EXP.1	The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (where possible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-1/2

Objective	Requirements Addressing the Objective	Rationale
		validation. FCS_BCM_EXP.1 is an explicit requirement that specifies the NIST FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensive the module is tested. FCS_CKM_EXP.2 Cryptographic Key Handling and Storage requires that FIPS PUB 140-1/2 be satisfied when performing key entry and output. FCS_CKM.4 mandates the standards (FIPS 140-1/2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. FCS_COP_EXP.1 requires that for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 140-1/2 standard.
O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE prior to permitting the use of any TOE services that require authentication.	FTA_TAB.1	FTA_TAB.1 meets this objective by requiring the TOE display a Security Administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the Security Administrator in which they specify any warnings regarding unauthorized use of the TOE and remove any product or version information if they desire. The only time that it is envisioned that an authenticated session would need to be established is for the performance of TOE administration. Bannering is not necessary prior to use of services that pass network traffic through the TOE.
O.DOCUMENTED_DESIGN	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1	ADV_FSP.1, ADV_HLD.1, ADV_RCR.1 supports this objective by requiring that the TOE be developed using sound engineering principles. The use of a high level design and the functional specification ensure that developers responsible for TOE development understand the overall design of the TOE. This in turn decreases the likelihood of design flaws and increases the chance that accidental design errors will be discovered. ADV_RCR.1 ensures that the TOE design is consistent across the High Level Design and the Functional Specification.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the	FMT_MSA.1 FMT_MSA.2 FMT_MSA.3-NIAP-0409 FMT_MOF.1(1)	The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirement's rationale for this objective focuses on the administrator's capability to perform management functions in order to control the

Objective	Requirements Addressing the Objective	Rationale
TOE, and restrict these functions and facilities from unauthorized use.	FMT_MOF.1(2) FMT_MTD.1	management functions in order to control the behavior of security functions. FMT_MSA.1, FMT_MSA.2 provides the Security Administrator the ability to accept only secure values and modify security attributes. FMT_MSA.3-NIAP-0409(1) requires that by default, the TOE does not allow an information flow, rather than allowing information flows until a rule in the rule set disallows it. FMT_MOF.1(1)(2) and FMT_MSA.3-NIAP-0409(2) are related to the services provided by FAU_UAU.1(1) and provide the Security Administrator control as to the availability of these services. FMT_MOF.1(1)(2) provides the ability to enable or disable the TOE services to the Security Administrator. FMT_MSA.3-NIAP-0409(2) requires that the these services by default are disabled. Since the Security Administrator must explicitly enable these services it ensures the Security Administrator is aware that they are running. This requirement does afford the Security Administrator the capability to override this restrictive default and allow the services to be started whenever the TOE reboots or is restarted. FMT_MOF.1(1) is used to ensure the administrators have the ability to invoke the TOE self-tests at any time. The ability to invoke the self-tests is provided to all administrators. The Security Administrator is able to modify the behavior of the tests (e.g., select when they run, select a subset of the tests). FMT_MOF.1(2) specifies the ability of the administrators to control the security functions associated with audit and alarm generation. The ability to control these functions has been assigned to the appropriate administrative roles. The requirement FMT_MTD.1 is intended to be used by the ST author, with possible iterations, to address TSF data that has not already been specified by other requirements. This is necessary because the ST author may add TSF data in assignments that cannot be addressed a priori by the PP authors.
O.MEDIATE The TOE must mediate the flow of information to and from wireless clients communicating via the TOE RF Transmitter/Receiver interface in accordance with its security policy.	FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1-NAIP-0407, FMT_SMF.1(3) FMT_SMF.1(5) FMT_MSA.3	FDP_IFC.1 and FDP_IFF.1-NIAP-0407 ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the sender.. FDP_IFC.1 provides the capability to set policy, while FDP_IFF.1-NIAP-0407 identifies the attributes that will be used to make policy decisions

Objective	Requirements Addressing the Objective	Rationale
		FMT_SMF.1(3), FMT_SMF.1(5) and FMT_MSA.3 ensure that the TOE provides an interface through which the information flow control policy can be set.
O.PARTIAL_FUNCTIONAL_TESTING The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	ATE_COV.1 ATE_FUN.1 ATE_IND.2	In order to satisfy O.PARTIAL_FUNCTIONAL_TESTING, the ATE class of requirements is necessary. ATE_FUN.1 requires the developer to provide the necessary test documentation to allow for an independent analysis of the developer's security functional test coverage. In addition, the developer must provide the test suite executables and source code, which the evaluator uses to independently verify the vendor test results and to support of the test coverage analysis activities. ATE_COV.1 requires the developer to provide a test coverage analysis that demonstrates the extent to which the TSFI are tested by the developer's test suite. This component also requires an independent confirmation of the extent of the test suite, which aids in ensuring that correct security relevant functionality of a TSFI is demonstrated through the testing effort. ATE_IND.2 requires an independent confirmation of the developer's test results, by mandating a subset of the test suite be run by an independent party. This component also requires an independent party to craft additional functional tests that address functional behavior that is not demonstrated in the developer's test suite. Upon successful completion of these requirements, the TOE's conformance to the specified security functional requirements will have been demonstrated.
O.RESIDUAL_ INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	FDP_RIP.1 FCS_CKM_EXP.2 FCS_CKM.4	FDP_RIP.1 is used to ensure the contents of resources are not available once the resource is reallocated. For this TOE it is critical that the memory used to build network packets is either cleared or that some buffer management scheme be employed to prevent the contents of a packet being disclosed in a subsequent packet (e.g., if padding is used in the construction of a packet, it must not contain another user's data or TSF data). FCS_CKM_EXP.2 places requirements on how cryptographic keys are managed within the TOE. This requirement places restrictions in addition to FDP_RIP.1, in that when a cryptographic key is moved from one location to another (e.g., calculated in some scratch memory and moved to a permanent location) that the memory area is immediately

Objective	Requirements Addressing the Objective	Rationale
		cleared as opposed to waiting until the memory is reallocated to another subject. FCS_CKM.4 applies to the destruction of cryptographic keys used by the TSF. This requirement specifies how and when cryptographic keys must be destroyed. The proper destruction of these keys is critical in ensuring the content of these keys cannot possibly be disclosed when a resource is reallocated to a user.
O.SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.	FPT_SEP.1 FPT_RVM.1	FPT_SEP.1 was chosen to ensure the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. FPT_RVM.1 ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to TOE resources (including TSF data and executable code) regardless of the defined policies. This includes controlling the accessibility to interfaces, as well as what access control is provided within the interfaces.
O.TIME_STAMPS The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.	FPT_STM.1	FPT_STM.1 requires that the TOE be able to provide reliable time stamps for its own use and therefore, partially satisfies this objective. Time stamps include date and time and are reliable in that they are always available to the TOE, and the clock must be monotonically increasing.
O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	FIA_UID.1 AVA_SOF.1 FIA_UAU.1	FIA_UID.1 plays a small role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions. In most cases, the identification cannot be authenticated (e.g., a user attempting to send a data packet through the TOE that does not require authentication. It is impractical to require authentication of all users that attempt to send data through the TOE, therefore, the requirements specified in the TOE require authentication where it is deemed necessary. This does impose some risk that a data packet was sent from an identity other than specified in the data packet. AVA_SOF.1 requires that any permutational or probabilistic mechanism in the TOE be analyzed be found to be resistant to attackers possessing a "low"

Objective	Requirements Addressing the Objective	Rationale
		attack potential. This provides confidence that security mechanisms vulnerable to guessing type attacks are resistant to casual attack. FIA_UAU.1 contributes to this objective by limiting the services that are provided by the TOE to unauthenticated users. Management requirements and the unauthenticated information flow policy requirement provide additional control on these services. In order to control logical access to the TOE an authentication mechanism is required. The local administrator authentication mechanism is necessary to ensure an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable).
O.VULNERABILITY_ ANALYSIS The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_VLA.1 AVA_SOF.1	AVA_VLA.1 requires the developer to perform a search for obvious vulnerabilities in all the TOE deliverables. The developer must then document the disposition of those obvious vulnerabilities. The evaluator then builds upon this analysis during vulnerability testing. This component provides the confidence that obvious security flaws have been either removed from the TOE or otherwise mitigated. AVA_SOF.1 requires that any permutational or probabilistic mechanism in the TOE be analyzed be found to be resistant to attackers possessing a “low” attack potential. This provides confidence that security mechanisms vulnerable to guessing type attacks are resistant to casual attack.

6.4 Rationale for TOE IT Environment Security Requirements

Table 14: Rationale for Requirements on the TOE IT Environment

Objective	Requirements Addressing the Objective	Rationale
OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information and the authentication credentials.	FAU_SAR.2 FAU_STG.1-NIAP-0429 FAU_STG.3 FMT_MOF.1	FAU_SAR.2 restricts the ability to read the audit records to only the Audit Administrator. The exception to this is that all administrative roles have access to the audit record information presented in the alarm indicating a potential security violation.

Objective	Requirements Addressing the Objective	Rationale
		FAU_STG.1-NIAP-0429 restricts the ability to delete or modify audit information to the administrators. The TSF will prevent modifications of the audit records in the audit trail. FAU_STG.3 ensures that the administrator will take actions when the audit trail exceeds pre-defined limits. FMT_MOF.1(1) is used to ensure the administrators have the ability to invoke the TOE self-tests at any time. The ability to invoke the self-tests is provided to all administrators. The Security Administrator is able to modify the behavior of the tests (e.g., select when they run, select a subset of the tests). FMT_MOF.1(2) specifies the ability of the administrators to control the security functions associated with audit and alarm generation. The ability to control these functions has been assigned to the appropriate administrative roles.
OE.AUDIT_REVIEW The IT Environment will provide the capability to selectively view audit information.	FAU_SAR.1 FAU_SAR.3	FAU_SAR.1 ensures that the IT environment provides those responsible for the TOE with facilities to review the TOE audit records (e.g., the Audit Administrator can construct a sequence of events provided the necessary events were audited). FAU_SAR.3 provides the Audit Administrator with the ability to selectively review the contents of the audit trail based on established criteria. This capability allows the Audit Administrator to focus their audit review to what is pertinent at that time.
OE.CRYPTANALYTIC Cryptographic methods used in the TOE shall be independently evaluated to be FIPS 140-1/2 compliant and will be shown to be resistant to cryptanalytic attacks (i.e. will be of adequate strength to protect unclassified Mission Support, Administrative, or Mission Critical data).	FCS_BCM_EXP.1 FCS_CKM_EXP.2 FCS_CKM.4 FCS_COP_EXP.1	The FCS requirements satisfy this objective by levying requirements that ensure the cryptographic standards include the NIST FIPS publications (where possible) and NIST approved ANSI standards. The intent is to have the satisfaction of the cryptographic standards be validated through a NIST FIPS 140-1/2 validation. FCS_BCM_EXP.1 is an explicit requirement that specifies the NIST FIPS rating level that the cryptographic module must satisfy. The level specifies the degree of testing of the module. The higher the level, the more extensive the module is tested. FCS_CKM_EXP.2 Cryptographic Key Handling and Storage requires that FIPS PUB 140-1/2 be satisfied when performing key entry and output.

Objective	Requirements Addressing the Objective	Rationale
		FCS_CKM.4 mandates the standards (FIPS 140-1/2) that must be satisfied when the TOE performs Cryptographic Key Zeroization. FCS_COP_EXP.1 requires that for data decryption and encryption that a NIST approved algorithm is used, and that the algorithm meets the FIPS PUB 140-1/2 standard.
OE.MANAGE The TOE IT environment will augment the TOE functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FAU_SAR.1 FAU_SAR.2 FIA_USB.1-NIAP-0415 FMT_MOF.1 FMT_SMR.1	FAU_SAR.1 ensures that the IT environment provides those responsible for the TOE with facilities to review the TOE audit records (e.g., the Audit Administrator can construct a sequence of events provided the necessary events were audited). FAU_SAR.2 ensures that the TOE IT environment will be capable of limit access to TOE audit records to only those with those users authorized to review them. FIA_USB.1-NIAP-0415 ensures that the TOE IT environment includes a mechanism to associate processes with roles. This ensures that both the TOE and its IT environment can identify FMT_MOF.1 ensures that the TOE IT environment limits access to TSF management functions to the administrator. FMT_SMR.1 ensures that the TOE IT environment provides an administrative role that may be used to manage both the TOE and the IT environment.
OE.NO_EVIL Sites using the TOE shall ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.	AGD_ADM.1	The AGD_ADM.1 requirement mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE and any security parameters that are configurable by the administrator. The documentation also provides a description of how to setup and review the auditing features of the TOE.
OE.PHYSICAL The IT environment provides physical security, commensurate with the value of the TOE and the data it contains.	A.Physical	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment. Therefore, an explicit requirement is not necessary.
OE.PROTECT_MGMT_COMMS The environment shall protect the	FDP_IFC.1(2) FDP_IFC.2 FDP_IFF.1-NIAP-	FDP_IFC.1(2) and FDP_IFF.1-NIAP-0407(2) ensure that the TOE has the ability to mediate packet flow based upon the authentication credentials of the

Objective	Requirements Addressing the Objective	Rationale
transport of audit records to the audit server, remote network management, and authentication server communications with the TOE in a manner that is commensurate with the risks posed to the network.	0407(2) FDP_ITT.1	sender. FDP_IFC.1 provides the capability to set policy for encryption to and from the wireless network, while FDP_IFF.1-NIAP-0407 identifies the attributes that will be used to make policy decisions. FDP_IFC.2 ensures that all possible operations and combinations are covered by the Wireless Encryption SFP and enforced by the TSF. FDP_ITT.1 ensures that data transferred internally between the TOE and IT Environment are protected through enforcement of the Wireless Encryption SFP and the Specified Users SFP.
OE.RESIDUAL_INFORMATION The TOE IT environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	FDP_RIP.1	FDP_RIP.1 ensures that the TOE IT environment provides same protections for residual information in a network packet that the TOE will provide. This ensures that neither the TOE nor the TOE IT environment will allow data from previously transmitted packets to be insert into new packets.

6.5 Rationale for Assurance Requirements

EAL2 augmented was chosen to ensure a confidence in security services used to protect information in a Basic Robustness Environment. The assurance selection was based on:

- Recommendations documented in the GIG; and
- The postulated threat environment.

The EAL definitions in Part 3 of the CC were reviewed and the *Basic Robustness Assurance Package* (Evaluation Assurance Level (EAL) 2 augmented with, ACM_SCP.1 (TOE CM Coverage), ALC_FLR.2 (Flaw Remediation), and AVA_MSU.1 (Misuse – Examination of Guidance).) was believed to best achieve this goal. The sponsor concluded that EAL2 augmented is applicable since this PP addresses circumstances where users require a basic level of independently assured security in commercial products. This level of assurance is commensurate with low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This collection of assurance requirements require TOE developers to gain assurance from good software engineering development practices which, do not require substantial specialist knowledge, skills, and other resources.

The postulated threat environment specified in Section 3 of this PP was used in conjunction with the Information Assurance Technical Framework (IATF) Robustness Strategy guidance to derive the chosen assurance level.

These three factors were taken into consideration and the conclusion was that the basic robustness assurance package was the appropriate level of assurance.

6.6 Rationale for Not Satisfying All Dependencies

Each functional requirement, including explicit requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. Table identifies the functional requirement, its correspondent dependency and the analysis and rationale for not supporting the dependency in this PP.

Table 15: Unsupported Dependency Rationale

Requirement	Unsatisfied Dependencies	Dependency Analysis and Rationale
FMT_MSA.2	ADV_SPM.1	The Government has determined that the requirement for the vendor to provide an informal TOE security policy model (ADV_SPM.1) is beyond basic robustness. Typically, this requirement is part of an EAL 4 requirement set. At basic robustness, there is no requirement for the vendor to model the security policies within this PP. Informal models of the Specified Users SFP and the Wireless Encryption SFP are contained within the PP, and are therefore not required to be provided by the vendor.
FPT_TST_EXP.1	FPT_AMT.1	This dependency is not necessary for this requirement because the FPT_AMT.1 is provided by the security objectives of the IT Environment.
FPT_TST_EXP.2	FPT_AMT.1	This dependency is not necessary for this requirement because the FPT_AMT.1 is provided by the security objectives of the IT Environment.

6.7 Rationale for Strength of Function Claim

Part 1 of the CC defines “strength of function” in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this PP. SOF-basic states, “a level of the TOE strength of function where analysis shows that the function provides adequate protection casual breach of TOE by attackers possessing a low attack potential.” The rationale for choosing SOF-basic was to be consistent with the TOE objective O.VULNERABILITY_ANALYSIS and assurance requirements included in this PP. Specifically, AVA_VLA.1 requires that the TOE be resistant obvious vulnerabilities, this is consistent with SOF-basic, which is the lowest strength of function metric. Consequently, security functions with probabilistic or permutational mechanisms chosen for inclusion in this PP were determined to adequately protect information in a Basic Robustness Environment. Similarly, probabilistic or permutational security functions included in any ST claiming conformance to this PP, must also meet an SOF Basic metric.

6.8 Rationale for Explicit requirements

Table 16 presents the rationale for the inclusion of the explicit requirements found in this PP.

Table 16: Rationale for Explicit Requirements

Explicit Requirement	Identifier	Rationale
FCS_BCM_EXP.1	Baseline cryptographic module	This explicit requirement is necessary since the CC does not provide a means to specify a cryptographic baseline of implementation.
FCS_CKM_EXP.2	Cryptographic key handling and storage	This explicit requirement is necessary since the CC does not specifically provide components for key handling and storage.
FCS_COP_EXP.1	Random number generation	This explicit requirement is necessary since the CC cryptographic operation components are focused on specific algorithm types and operations requiring specific key sizes.
FCS_COP_EXP.2	Cryptographic Operation	This explicit requirement is necessary because it describes requirements for a cryptomodule rather that the entire TSF.

Explicit Requirement	Identifier	Rationale
FPT_TST_EXP.1	TSF Testing	This explicit requirement is necessary because, as identified in the US Government PP Guidance for Basic Robustness, there are several issues with the CC version of FPT_TST.1. First, the wording of FPT_TST.1.1 appears to make sense only if the TOE includes hardware; it is difficult to imagine what software TSF "self-tests" would be run. Secondly, some TOE data are dynamic (e.g., data in the audit trail, passwords) and so interpretation of "integrity" for FPT_TST.1.2 is required, leading to potential inconsistencies amongst Basic Robustness TOEs. Therefore, the explicit requirements are used in this PP.
FPT_TST_EXP.2	Testing of cryptographic modules	This explicit requirement is necessary because the basic self test requirement does not specify the required elements for testing of cryptographic functions, as called out in this explicit requirement.

Appendix A. Acronyms

AES	Advanced Encryption Standard
AP	Access Point
ASCII	American Standard Code for Information Interchange
CC	Common Criteria
CM	Configuration Management
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GIG	Global Information Grid
HARA	High-Assurance Remote Access
I&A	Identification and Authentication
IATF	Information Assurance Technical Framework
IGS	Installation Generation Startup
ISSE	Information System Security Engineers
IT	Information Technology
NIST	National Institute of Standards and Technology
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
PUB	Publication
RF	Radio Frequency
SBU	Sensitive But Unclassified
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SoF	Strength of Function
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network